AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# IDENTITY THEFT AND TAX FRAUD: GROWING PROBLEMS FOR THE INTERNAL REVENUE SERVICE

## HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY AND FINANCIAL MANAGEMENT

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

NOVEMBER 4, 2011

**Serial No. 112–96**

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

72–798 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

## COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
CONNIE MACK, Florida
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
ANN MARIE BUERKLE, New York
PAUL A. GOSAR, Arizona
RAÚL R. LABRADOR, Idaho
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
JOE WALSH, Illinois
TREY GOWDY, South Carolina
DENNIS A. ROSS, Florida
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas
MIKE KELLY, Pennsylvania

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
EDOLPHUS TOWNS, New York
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
DANNY K. DAVIS, Illinois
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
CHRISTOPHER S. MURPHY, Connecticut
JACKIE SPEIER, California

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
ROBERT BORDEN, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

### SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY AND FINANCIAL MANAGEMENT

TODD RUSSELL PLATTS, Pennsylvania, *Chairman*

CONNIE MACK, Florida, *Vice Chairman*
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas

EDOLPHUS TOWNS, New York, *Ranking Minority Member*
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
ELEANOR HOLMES NORTON, District of Columbia

# CONTENTS


| | Page |
|---|---|
| Hearing held on November 4, 2011 | 1 |
| Statement of: | |
| George, J. Russell, Treasury Inspector General for Tax Administration; Steven T. Miller, Deputy Commissioner for Services and Enforcement, Internal Revenue Service; and Ronald A. Cimino, Deputy Assistant Attorney General for Criminal Matters, Tax Division, U.S. Department of Justice | 12 |
| Cimino, Ronald A. | 29 |
| George, J. Russell | 12 |
| Miller, Steven T. | 41 |
| Nugent, Hon. Richard B., a Representative in Congress from the State of Florida | 5 |
| Letters, statements, etc., submitted for the record by: | |
| Cimino, Ronald A., Deputy Assistant Attorney General for Criminal Matters, Tax Division, U.S. Department of Justice, prepared statement of | 31 |
| George, J. Russell, Treasury Inspector General for Tax Administration, prepared statement of | 15 |
| Miller, Steven T., Deputy Commissioner for Services and Enforcement, Internal Revenue Service, prepared statement of | 43 |
| Nugent, Hon. Richard B., a Representative in Congress from the State of Florida, prepared statement of | 8 |
| Towns, Hon. Edolphus, a Representative in Congress from the State of New York, prepared statement of | 4 |

# IDENTITY THEFT AND TAX FRAUD: GROWING PROBLEMS FOR THE INTERNAL REVENUE SERVICE

---

**FRIDAY, NOVEMBER 4, 2011**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT ORGANIZATION,
EFFICIENCY AND FINANCIAL MANAGEMENT,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
*Washington, DC.*

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2154, Rayburn House Office Building, Hon. Todd Platts (chairman of the subcommittee) presiding.

Present: Representatives Platts, Towns, and Connolly.

Also present: Representative Nugent.

Staff present: Michael R. Bebeau, assistant clerk; Molly Boyl, parliamentarian; Mark D. Marin, director of oversight; Tegan Millspaw, research analyst; James Robertson, professional staff member; Beverly Britton Fraser, minority counsel; Ashley Etienne, minority director of communications; Jennifer Hoffman, minority press secretary; and Adam Koshkin, minority staff assistant.

Mr. PLATTS. The committee will come to order.

I appreciate everyone's attendance here today. I do apologize with—I know I'm going to be challenged with scheduling conflicts. I know on our side of the aisle a House Republican Conference that was scheduled unfortunately for the exact same time on the balanced budget amendment at the last minute. But we are glad to have everyone's participation with all of our witnesses.

Today's hearing is a continuation of the subcommittee's examination of the serious problem of tax fraud across the country. In June, this subcommittee held a hearing on tax fraud perpetrated by identify theft. We heard testimony from three witnesses who had their identities and tax returns stolen. This hearing will address recent developments in tax fraud and evaluate the government's efforts to identify and prevent fraud.

Tax fraud is a rapidly growing problem, and identity theft related fraud is particularly concerning. In order to steal someone's tax return, all the perpetrator of this type of fraud needs is a name and a Social Security number. This information is then used to submit a fraudulent claim. If a victim has not filed taxes yet, the criminal is even able to steal the victim's tax return.

In 2008, the Internal Revenue Service identified over 50,000 cases of identity theft related fraud. In 2010, that number had in-

creased to approximately 248,000. Many cases go undetected, and the actual number of identity theft tax fraud could be much higher.

Identity thieves obtain personal information from many sources, including doctors' offices, school systems, and human resources departments. Some thieves get information from the Social Security death index and file fraudulent claims under the names of deceased individuals. In 2010, IRS paid over $12 million to people who were listed as deceased. Service members who were killed in action defending this great Nation are often targets of identity thieves who use their information to steal tax returns from their families.

Tax credit fraud is another growing problem. The Treasury Inspector General for Tax Administration found that in 2010 IRS issued $4.2 billion in tax credits to individuals who were unauthorized to work in the United States. IRS has not recovered that money.

Additionally, TIGTA discovered that IRS improperly issued approximately $3.2 billion in educational tax credits. Some of those educational credits went to prisoners.

Although tax fraud is a serious crime, it is difficult to investigate or prosecute the perpetrators of these crimes. All potential cases are reviewed by the Department of Justice and must be approved before IRS can investigate. IRS also has limited resources to investigate criminal activity and rarely investigates tax return fraud because the average amount per return is $3,400.

While this is a small number, it can be devastating to the victims who had their identities and tax returns stolen. It also quickly adds up to millions of dollars of improper payments each year that go to criminals.

IRS has been working to address the increasingly serious problem of tax fraud, and it deserves credit for its efforts. However, more must be done to address this issue.

Today, we will hear from our witnesses about the process of investigating tax fraud and IRS's work with the Department of Justice to prosecute the perpetrators of this fraud. We will also learn about the work IRS and TIGTA are doing to better identify and prevent fraud before it occurs.

I certainly thank our witnesses in advance for their testimony here today and the written testimony they have supplied, and I would emphasize that a lot of our focus here today is going to be about protecting taxpayers' money so that we don't lose money to this type of fraud.

But a very important aspect of our June hearing and again today is the fact that this is how—we want to focus on how the Federal Government is protecting American taxpayers against these crimes and how we then assist the victims of these crimes when they occur and that we not lose sight of the fact, you know, that this is the real lives of American citizens, law-abiding citizens, that are tremendously impacted when tax identity fraud occurs.

With that, I'll yield to my distinguished colleague, the ranking member of the subcommittee from New York, Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman, for holding this hearing on identity theft and tax fraud, growing problems, of course, which we have been dealing with now for—this is the second time, the second hearing.

In 2011 alone, the IRS has already identified over 582,000 taxpayers that were the subject of identity theft, and this is more than double the incidence from only 3 years ago. Clearly, we have to do a better job protecting the taxpayer and the Treasury from criminals. Our witnesses today will help us understand how this can be done.

One of the first priorities we must address is the quality of assistance given to taxpayers victimized by employment or tax refund fraud. The testimony does not paint a pretty picture of how the IRS is handling this aspect of its responsibilities. It is unacceptable to have innocent taxpayers waiting 12 to 18 months to verify their identity before a replacement refund check is issued. We can and should do better.

Another obvious problem is what is being done to prevent criminals from filing fraudulent tax returns using stolen identification? I fully understand that identities are stolen, traded, and misused in places far away from the IRS. It is also clear that neither the IRS nor law enforcement nor anyone else can predict when criminal behavior will occur or stopping criminals bent on breaking the law. However, if there are resources, both human and technological, to prevent criminals from filing fraudulent returns, every effort should be made to do so.

If the IRS, the Inspector General, or the Department of Justice does not enforce the law against those who defraud the Treasury and victimize taxpayers to identity theft, there will be no deterrent or punishment for criminals.

I hear of budgetary limitations, staff limitations, a lack of training programs, and legal limitations that prevent more investigations and prosecution of these crimes. We cannot sit back and do nothing because of limitations. The criminals are becoming more sophisticated in defrauding the government. We have to become more creative in our solutions. Because if they find out that we cannot do anything about it, that means that the numbers that we just talked about earlier will continue to increase.

I look forward to the testimony today. I hope our witnesses will guide us through the present limitations to working solutions against the problem of identity theft and tax fraud. And let me just say to all the witnesses that, you know, this committee is not an "I got you" committee. You know, some of the committees around here are the "I got you" committee, and they want to get you.

But we're not here to do that. We want to be the "help you" committee, to be able to make certain that people who are having problems, that there is a solution to the problem within a quick period of time and to prevent the problem from continuing to grow.

So thank you very much.

Representative Nugent, good to see you here as well.

[The prepared statement of Hon. Edolphus Towns follows:]

**Opening Statement**
**Rep. Edolphus Towns, Ranking Member**
**Hearing on "Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service"**
**Subcommittee on Government Organization, Efficiency and Financial Management**

**November 4, 2011**

Today's hearing is the second part of this committee's examination of how the IRS handles the growing problem of identity theft and tax fraud. In 2011 alone, the IRS has already identified over 582,000 taxpayers that were the subject of identity theft and this is more than double the incidents from only 3 years ago. Clearly we have got to do a better job protecting the taxpayer and the treasury from criminals. Our witnesses today will help us understand how this can be done.

Thank you Inspector General, George, Mr. Miller, and Mr. Cimino for your appearances and testimony today. The three of you have front seats to the arena of identity theft crimes as it affects tax administration. You are uniquely positioned to evaluate the system and suggest meaningful changes that can help the government win the war against this crime.

One of the first priorities we must address is the quality of assistance given to taxpayers victimized by employment or tax refund fraud. The testimony does not paint a pretty picture of how the IRS is handling this aspect of its responsibilities. It is unacceptable to have innocent taxpayers waiting 12 to 18 months to verify their identity before a replacement refund check is issued. We can and should do better.

Another obvious problem is what is being done to prevent criminals from filing fraudulent tax returns using stolen identification. I fully understand that identities are stolen, traded, and misused in places far away from the IRS. It is also clear that neither the IRS nor law enforcement nor anyone else can predict when criminal behavior will occur or stop a criminal bent on breaking the law. However, if there are resources, both human and technological, to prevent criminals from filing fraudulent returns, every effort should be made to do so.

If the IRS, the Inspector General or the Department of Justice does not enforce the law against those who defraud the treasury and victimize taxpayers through identity theft, there will be no deterrent or punishment for criminals. I hear of budgetary limitations, staffing limitations, and legal limitations that prevent more investigations and prosecutions of these crimes. We cannot sit back and do nothing because of limitations. The criminals are becoming more sophisticated in defrauding the government. We have to become more creative in our solutions.

I look forward to the testimony today. I hope our witnesses will guide us through the present limitations to working solutions against the problem of identity theft and tax fraud.

Mr. PLATTS. The gentleman yields back.

And certainly I fully agree with the ranking member that our purpose and assignment here is to partner with our colleagues in the House, our colleagues throughout the Federal Government on how we can well serve our fellow constituents, our joint constituents, all Americans, and to get a good result, not to play gotcha but to just work with you to get good results.

We are honored to join with—not a member of our committee but another colleague—a distinguished Member of our freshman class here in Congress, Congressman Rich Nugent of Florida's Fifth District.

Congressman, we're honored to have your testimony as one who's seen the challenge of tax fraud firsthand in your district. I know you're going to share that story with all of our guests here today.

Mr. Nugent was sheriff of Hernando County, Florida, prior to joining Congress so brings perspective not just as a Member of the House but also as a long-time dedicated law enforcement official.

So, Rich, we're delighted to have you here with us; and you're recognized for a statement.

**STATEMENT OF HON. RICHARD NUGENT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA**

Mr. NUGENT. Thank you, Mr. Chairman.

First, I want to take just a moment to thank the subcommittee and especially Chairman Platts and Ranking Member Towns for the opportunity to speak here today.

Although tax fraud and identity theft is a nationwide problem, I want to make the subcommittee aware of what's happening in the Tampa Bay area in my district. Recently, Tampa Bay—or Tampa Police Department started noticing that many of their most notorious drug dealers were no longer on the street. Officers pulled one of their previous dealers over during a routine traffic stop and discovered massive amounts of prepared debit cards, ledgers containing Social Security numbers, and laptop computers in the back of the car.

Through this and similar routine traffic stops and drug busts, Tampa Police Department discovered a scheme known as Turbo Tax. One perpetrator had a ledger containing 100 names of deceased people, and after the investigation it was discovered that this man had made well over 1,000 false returns and collected close to $2.4 million.

The Tampa Police Department worked well with the local IRS agents and U.S. attorneys in their investigations. However, once they went to the D.C. bureaucrats detailing exactly how criminals steal the Social Security numbers, file the fraudulent tax returns, and launder resulting money, the Feds mostly turned a blind eye to that issue.

Tampa PD have explained how the criminals got Social Security numbers. Initially, they targeted deceased people, filing returns, information they found on Web sites, like Ancestry.com. Once they ran out of dead folks, they started stealing Social Security numbers from living victims. Tampa Police Department has had cases where information was stolen from nursing homes, schools, and hospitals. Additionally, James Haley VA Medical Center sent letters to about

200 veterans warning them that their identity had been stolen to file false tax returns. The VA Inspector General is investigating this case currently.

Tampa Police Department also knows how the criminals are filing the their returns. The actual fraud is not committed by an organized group but by individuals. Tampa Police Department has busted what the lawbreakers call "make it rain parties" where criminals get together in a hotel room with Internet access and file fake return after fake return.

Police know how the money's being laundered. The criminals have worked out deals with unscrupulous business owners who cash their checks or debit cards in exchange for a cut of the money.

In Tampa, the most money seems to be laundered by a select group of high-cash-flow businesses, including used car dealers and clothing shops. One business alone received approximately $3.5 million in Treasury money, our money.

How does Tampa Police Department know all this? The criminals are telling them. Even after they have been read their Miranda rights, the crooks are laying out their entire process to the cops. They are freely admitting their crimes because they don't think Federal officials would do anything about it; and, unfortunately, it seems the criminals are right.

As a representative from GAO told the subcommittee in your June hearing on this issue, IRS identified 248,357 incidents of tax-related identity theft in 2010. However, the IRS Criminal Investigative Division only had 4,706 active investigations into all types of fraud.

The IRS and the Justice Department say that these cases aren't of sufficient severity for them to look into. Experiences in Tampa show the lack of action is not reflective of the agents' desire across the ground to prosecute but the bureaucracy within the IRS and their administrators.

Even more infuriating is the Federal agencies are notifying the IRS of this fraud, but they continue to send checks. In Tampa alone, the U.S. Postal Service stopped delivery of an estimated $100 million in fraudulent refunds in a 6-month period.

Media reports also say the company issuing of prepaid debit cards notified the IRS of concerns. However, the IRS ignored those warnings and just sent Treasury checks to those suspected fraudsters.

I cannot understand how other government offices can be telling the IRS that their checks are going to fraudsters and yet the IRS continues to pump them out. Given our current fiscal situation, it's unconscionable that the Federal Government can be aware of billions of dollars in tax dollars being stolen right out from under our noses and do very little about it.

I'm here because I want to find a solution to the problem. First, the IRS needs better controls to keep the fraudulent returns from ever going out the door. Second, when identity related fraud does occur, these criminals must be prosecuted, and local law enforcement ought to be involved in the process.

Maybe the IRS doesn't want to increase anti-fraud safeguards because it might slow down the return process, but I think honest

taxpayers would rather get the returns a few days later and keep the money out of the hands of criminals and get their tax return.

In closing, thank you again, Chairman Platts, for the opportunity to testify this morning. I look forward to working with both Federal and local officials, as well as my colleagues in Congress, including the subcommittee, to bring an end to this needless waste of taxpayer dollars.

[The prepared statement of Hon. Richard Nugent follows:]

November 4, 2011

Rep. Rich Nugent (FL-5)

**Testimony of Rep. Richard Nugent Before the**

**Committee on Oversight and Government Reform**

**Subcommittee on Government Organization, Efficiency, and Financial Management**

First, I want to take a moment to thank the Subcommittee and especially Chairman Platts and Ranking Member Towns for the opportunity to speak before you today. Although tax fraud identity theft is a nationwide problem, I wanted to make the Subcommittee aware of what's happening in Tampa Bay area and my District.

Recently, the Tampa PD started noticing that many of their most notorious drug dealers were no longer on the streets. Officers pulled one of their previous dealers over during a routine traffic stop and discovered massive amounts of prepaid debit cards, ledgers containing Social Security numbers, and laptop computers in the back of the car.

Though this and similar routine traffic stops and drug busts, Tampa PD discovered a scheme known as "Turbo Tax." One perpetrator had a ledger containing 100 names of deceased people and, after investigations, it was discovered that this one man had made well over 1,000 false returns and had collected $2.4 million.

Tampa PD worked well with local IRS agents and U.S. Attorneys in their investigations. However, once they went to the D.C. bureaucrats, detailing exactly how the criminals steal the Social Security numbers, file the fraudulent tax returns, and launder the resulting money, the feds mostly turned a blind eye to the fraud.

The Tampa PD have explained how the criminals got Social Security numbers. Initially, they targeted deceased people, filing returns with information they found on websites like ancestory.com . Once they ran out of dead people, they started stealing Social Security Numbers from living victims. Tampa Police Department has had cases where information was stolen from nursing homes, schools, and hospitals. Additionally, James Haley VA Medical Center sent letters to about 200 veterans warning them that their identity had been stolen to file false tax returns. The VA Inspector General is investigating this case.

Tampa PD also knows how the criminals are filing the returns. The actual fraud is not committed by an "organized group" but by individuals. The Tampa PD have busted what the lawbreakers call "Make It Rain Parties," where criminals get together, get a hotel room with internet access, and file fake return after fake return.

The police know how the money's being laundered. The criminals have worked out deals with unscrupulous business owners who cash the checks or the debit cards in exchange for a cut of the money. In Tampa, most of the money seems to be laundered by a select group of high cash flow

businesses including used car dealers and clothing shops. One business alone received approximately $3.5 million in Treasury money.

How does Tampa PD know all of this? The criminals are telling them.

Even after they've been read their Miranda Rights, the crooks are laying out their entire process to the cops. They're freely admitting their crimes, because they don't think federal officials will do anything about it. Unfortunately, it seems the criminals are right.

As a representative from the GAO told the Subcommittee in your June hearing on this issue, the IRS identified 248,357 incidents of tax-related identity theft in 2010. However, in 2010, the IRS Criminal Investigative division only had 4,706 investigations total, into all types of fraud. The IRS and by the Justice Department just say these cases aren't of "sufficient severity" for them to look into it. Experiences in Tampa show that the lack of action is not reflective of the agents' desire to prosecute, but the bureaucracy within the IRS and their administrators.

Even more infuriating, other federal agencies are notifying the IRS of this fraud, but they continue to send the checks. In Tampa alone, the U.S. Postal Service stopped the delivery of an estimated $100 million in fraudulent refunds in a six-month period. Media reports also say that the company issuing the prepaid debit cards notified the IRS of fraud concerns. However, the IRS ignored these warnings and just sent out Treasury checks to those suspected fraudsters. I cannot understand how other government offices can be telling the IRS that their checks are going to fraudsters, and yet the IRS continues to pump them out.

Given our current fiscal situation, it is unconscionable that the federal government can be aware of billions of dollars of tax dollars being stolen right out from under our noses and do very little about it.

I'm here because I want to find a solution to this problem. First, the IRS needs better controls to keep these fraudulent returns from ever going out the door. Second, when identity-related tax fraud does occur, these criminals must be prosecuted, and local law enforcement ought to be involved in that process.

Maybe the IRS doesn't want to increase anti-fraud safeguards because it might slowdown the return process. But I think honest taxpayers would rather get their returns a few days later, and keep money out of the hands of criminals, than get their tax return a day or two faster.

In closing, thank you again, Chairman Platts, for the opportunity to testify this morning. I look forward to working with both federal and local officials as well as my colleagues here in Congress, including the Subcommittee, to bring an end to this needless waste of taxpayer dollars.

Mr. PLATTS. Congressman Nugent, we certainly thank you for your testimony and especially your personal insights into this challenge that we're trying to deal with with the IRS both in your district as well as your background in law enforcement. You bring a great level of expertise to assist this subcommittee in our efforts.

We're not just glad to have your testimony but ask unanimous consent that Mr. Nugent will join us on the dais and be part of the hearing for Q&A is as well.

Mr. NUGENT. Thank you very much.

Mr. PLATTS. We will reset for our second panel and certainly honored to have three distinguished witnesses with us here today.

First, the Honorable J. Russell George, Treasury Inspector General for Tax Administration. This is a little bit of a homecoming for Mr. George as former staff director under a distinguished, now passed on, chairman, Steve Horn of this very subcommittee from, I think, the mid-'90's to about 2002.

Mr. George, we're delighted to have you back and have you both as an alumnus of the subcommittee staff and also your current work as Treasury Inspector General for Tax Administration.

Also delighted to have Mr. Ron Cimino—I will try to make sure I get that correct for you—Deputy Assistant Attorney General for the Tax Division at the U.S. Department of Justice; and the distinguished Steven Miller, Deputy Commissioner for Enforcement at the Internal Revenue Service.

Now that you're all three seated, if I could ask you to rise. The practice of the full and all of our subcommittees here is to swear in our witnesses.

If you would raise your right hands.

[Witnesses sworn.]

Mr. PLATTS. Let the clerk reflect that the witnesses all answered in the affirmative.

We are going to do our best to be efficient with your time. It's our understanding that we're going to have votes on the floor somewhere in the next half hour to 45 minutes, hopefully closer to an hour; and our hope is we can get your oral testimony here today. We have your written testimony and then get to Q&A with members of the committee and not have you wait too long, if at all, based on floor votes.

So if you can try to limit your testimony, written—your oral testimony to 5 minutes and then allow us to get into a good exchange as part of the Q&A.

So, Mr. George, if you would like to begin.

## STATEMENTS OF J. RUSSELL GEORGE, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION; STEVEN T. MILLER, DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT, INTERNAL REVENUE SERVICE; AND RONALD A. CIMINO, DEPUTY ASSISTANT ATTORNEY GENERAL FOR CRIMINAL MATTERS, TAX DIVISION, U.S. DEPARTMENT OF JUSTICE

### STATEMENT OF J. RUSSELL GEORGE

Mr. GEORGE. Thank you, Mr. Chairman—Chairman Platts, Ranking Member Towns, Mr. Nugent. Thank you for the invitation

to testify on the issue of identity theft and tax refund and tax fraud.

There are two primary types of identity theft that relate to tax administration. The first involves an individual using another person's name and/or Social Security number to file a fraudulent tax return to generate a tax refund, which I will refer to as a tax fraud identity theft. The second involves using another person's identity, for example, the names, Social Security number, or both, to obtain employment, which I will refer to as employment-related identity theft.

In 2008, TIGTA recommended that the IRS develop and implement a strategy to address both of these types of identity theft. Since then, the number of tax-related identity theft incidents has grown significantly.

Although the IRS acknowledges that it does not know the exact number of open or closed identity theft cases, as of August 31st of this year IRS incident tracking reports indicated that the number of taxpayers affected by identity theft has more than doubled since 2008 to over 580,000 taxpayers this year alone.

TIGTA is currently evaluating whether the IRS has effectively provided assistance to victims of identity theft. Our preliminary observations are that the IRS' processes are not adequate to communicate identity theft procedures to taxpayers. This results in increased burden for these victims.

We have analyzed recent identity theft cases and found that the IRS' process for assisting victims is very lengthy. As was pointed out earlier, a typical path for an identity theft refund case that is not complex may take as long as 18 months to resolve.

Standard IRS processes and organizational structure hinder timely and effective case resolution. High telephone call demand, limited resources, and a growing identity theft inventory make it difficult for customer service assisters to prioritize identity theft cases. The assisters who work the majority of identity theft cases also work the IRS' toll-free telephone number responding to telephone taxpayer inquiries.

Identity theft cases are not always a priority even though an untimely case resolution could result in significant taxpayer burden as well as an improper payment. Identity theft case processing is highly decentralized, and coordination among the IRS functions is limited.

Procedures pertaining to identity theft are not arranged for efficient access. They are inconsistent and are scattered throughout the Internal Revenue manual.

The different systems used by the various functions prevent accurate tracking and reporting of identity theft workloads and their effect on tax administration. There is no mechanism or system in place to track cases in process or time spent working cases.

Total time spent on a case can vary significantly, and sometimes cases can stay open for months with little or no activity as the assisters answer calls or work other types of cases.

In fiscal year 2011, the IRS began issuing identity protection Personal Identification Numbers, referred to as PINs, to tax payers who have been previously identified by the IRS as victims of identity theft. The PIN will indicate the taxpayer provided the IRS

with information that validates their identity and that the IRS is satisfied the taxpayer is the valid holder of the Social Security number.

Currently, the IRS provides the identity protection PINs only to taxpayers who have been a victim of identity theft that has affected the filing or processing of their Federal tax return. The PIN is not available to taxpayers who claim to have been a victim of identity theft but who have not had problems filing their tax returns.

While the financial sector offers customers the option of providing additional protection on their accounts, the IRS should consider adopting such practices. Providing protection only after the taxpayer has been victimized does not serve the American taxpayer well.

A substantial number of unscrupulous taxpayers submit fraudulent tax returns to the IRS for the sole purpose of receiving a tax refund. From January 1st through September 10th of this year, the IRS reported that it received over 1.6 million tax returns with more than $12 billion claimed in fraudulent tax refunds, and yet it prevented the issuance of $11.5 billion of that money.

Tax-related identity theft is a growing concern despite the IRS' efforts to address this serious problem. It is critical for the IRS to deter and detect identity theft before it occurs within the tax return process. The IRS needs a better process to identify and respond whenever identity theft fraud occurs.

While the IRS has undertaken important steps and initiatives to prevent the occurrence of identity theft, additional controls could minimize and prevent future incidences.

Thank you, Mr. Chairman for the opportunity to present testimony.

[The prepared statement of Mr. George follows:]

TESTIMONY OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
*before the*
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT ORGANIZATION,
EFFICIENCY AND FINANCIAL MANAGEMENT
U.S. House of Representatives

"Identity Theft and Tax Fraud"

November 4, 2011

Chairman Platts, Ranking Member Towns and Members of the Subcommittee, thank you for the invitation to speak before you today on the subject of identity theft and its impact on the Internal Revenue Service's (IRS) function of administering the Nation's tax laws. My comments will focus on the ongoing work that the Treasury Inspector General for Tax Administration (TIGTA) has underway to evaluate the IRS's efforts in identifying and preventing identity theft relating to tax administration and to assist taxpayers who have been victims of identity theft.

There are two primary types of identity theft that relate to tax administration: the first type involves an individual using another person's name and/or Social Security Number (SSN) to file a fraudulent tax return to generate a tax refund. I will refer to this form of identity theft as "tax fraud identity theft." The second type involves using another person's identity (*e.g.,* name, SSN, or both) to obtain employment. I will refer to this form of identity theft as "employment-related identity theft."

In April 2008, I testified on the growing threat of identity theft to tax administration. At that time, we reported that the IRS had not placed sufficient emphasis on developing strategies to address either form of identity theft, whether employment- or tax-fraud-related. The IRS lacked the comprehensive data needed to determine the impact of identity theft on tax administration. Its prevention strategy did not include pursuing individuals using another person's identity, unless a case directly related to a substantive tax violation. According to IRS policy at that time, identity theft crimes were investigated by the IRS's Criminal Investigation Division if the crime was committed in conjunction with other criminal offenses having a large tax effect.

In 2008, TIGTA recommended that the IRS develop and implement a strategy to address both employment-related and tax-fraud identity theft.[1] We recommended that this strategy include coordinating with other Federal agencies, such as the Federal Trade Commission and Social Security Administration, to evaluate and investigate identity-theft allegations related to tax administration. We also recommended improvements in the use of an identity theft closing codes in the IRS's compliance functions.[2]

At that time, it was the IRS's position that it did not have sufficient enforcement resources to address most identity-theft cases. Moreover, it stated that employment-related identity theft cases were not the responsibility of the IRS and that it would not be worthwhile to pursue employment-related identity theft cases for unreported tax liabilities because the taxes owed on most of these cases were not significant. We expressed concern that if the IRS did not take additional action to stem the problem, there would be no deterrent effort to keep the problem from spreading.

Since 2008, the number of tax-related identity-theft incidents impacting tax administration has grown significantly. Although the IRS acknowledges that it does not know for certain the number of open or closed identity-theft cases, as of August 31, 2011, IRS incident tracking reports indicate that 582,736 taxpayers were affected by identity theft in Calendar Year 2011. In Calendar Year 2008, the IRS reported 254,079 taxpayers were affected.

**IRS's Assistance to Victimized Taxpayers**

The impact of identity theft on taxpayers is profound and can have major consequences. Employment-related identity theft can affect taxpayers when the IRS attempts to take enforcement actions for what appears to be unreported income. Refund fraud using another person's identity has a more substantial effect. After an identity thief has successfully committed this crime and is enjoying the benefits, the victim begins to realize the harm. It affects lawful taxpayers' ability to file their tax returns and can significantly delay their tax refunds.

TIGTA is currently evaluating whether the IRS is effectively providing assistance to victims of identity theft.[3] To date, auditors have analyzed identity theft cases, reviewed all significant guidance and procedures dealing with identity theft, and conducted interviews with more than 200 IRS employees who work identity theft issues. TIGTA interviewed employees in all aspects of the Identity Theft Program, including assistors, technicians, case reviewers, quality team

[1] TIGTA, Ref. No. 2008-40-086, *Outreach Has Improved, But More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft* (March 2008).
[2] A closing code is entered on an account when the case is closed and identifies the type of case.
[3] TIGTA, Audit No. 201140042, *Effectiveness of Assistance Provided to Victims of Identity Theft* (planned report issuance in May 2012).

managers, production monitors, tax examiners, analysts, managers, and executives.

Our preliminary observations are that the IRS is not effectively providing assistance to victims of identity theft and its processes are not adequate to communicate identity-theft procedures to taxpayers. This results in increased burden for the victims of identity theft.

We have analyzed recent identity theft cases to evaluate the IRS process for assisting victims and have found that the process is very lengthy. While we cannot provide specific case examples due to privacy and disclosure laws, the following timeline illustrates a composite for an identity theft refund fraud case.

**February** The identity thief files a fraudulent tax return and obtains a tax refund. Subsequently, the lawful taxpayer attempts to electronically file his tax return, for which he is due a tax refund. He receives an IRS rejection notice stating that his SSN cannot be used more than once on the tax return or on another tax return.

The taxpayer calls the IRS toll-free telephone line and explains the situation to the customer service assistor. The assistor, after authenticating the taxpayer, researches his tax account and determines a tax return has already been filed using that name and SSN. The assistor advises the taxpayer to file a paper tax return, attaching an Identity Theft Affidavit (Form 14039, which is attached to the testimony) or a police report and a valid government-issued document such as a copy of a Social Security card, passport, or driver's license to the tax return and mail it to the IRS.

The IRS receives the paper tax return in one of its processing sites and a technician enters the data into the IRS's computer system.[4] It is rejected. A technician determines it is a duplicate tax return and inputs the appropriate transaction code. The duplicative return case is received in the Duplicate function, where an assistor identifies this as a possible identity theft case. The assistor requests the paper tax return. The case is set aside in a queue to be worked after April 15, when the filing season has ended.

**April** The taxpayer calls the IRS toll-free line again and asks when he will receive his tax refund. The assistor researches the taxpayer's account, determines a duplicate tax return has been filed, and advises the taxpayer that there will be processing delays and he may receive correspondence requesting additional information. The assistor also advises the taxpayer to visit the IRS's website at IRS.gov for additional information and links related to identity theft.

**July** The taxpayer's tax return is worked in the Duplicate Function and determined to be an identity theft case. The duplicative tax return is transferred to another unit to an assistor whose responsibilities also include answering IRS toll-free telephone calls. The case is scanned into a management information system and queued.

**September** The assistor begins working the case, orders copies of original tax returns, and sends letters to the alleged identity thief and the taxpayer to attempt to determine who the legitimate taxpayer is. The legitimate taxpayer responds, confirming that he did not file the first tax return the IRS received.

---

[4] The paper tax return with all attachments is sent to the Files Unit, which is a repository where paper tax returns and related documents are stored.

**October** The taxpayer calls the Identity Protection Specialized Unit and asks when he should expect his tax refund. The assistor researches the case and advises him his case is being worked. The customer service representative sends a referral to the assistor working the case.

**November** The assistor determines which is the legitimate taxpayer, requests adjustments to the taxpayer's account, and sends a letter to the identity thief providing him or her with a temporary tax identity number and a letter to the legitimate taxpayer advising him he has been a victim of identity theft and his account has been flagged.

**December** The legitimate taxpayer receives the letter from the IRS and calls the Identity Protection Specialized Unit to inquire when he will receive his tax refund. The assistor advises him that it has been scheduled.

**January** The adjustments post to the legitimate taxpayer's account and the refund is released. He receives another letter advising him he has been a victim of identity theft and his account has been flagged. A tax account for the person who committed the identity theft is also established.[5]

The above illustration provides a "best case" resolution of an identity theft case. However, most cases are more complex and can present considerable challenges throughout the resolution process. For instance, it can be difficult to determine who the legitimate taxpayer is or if the case is actually a case of identity theft. Taxpayers sometimes transpose digits in SSNs, but do not respond to the IRS when it requests information to resolve the case. As a result, the IRS may not be able to determine who the legitimate taxpayer is. With other cases we have reviewed, taxpayers claimed to be victims of identity theft after receiving refunds for which the IRS had questioned deductions or credits or proposed examination adjustments. In certain instances, the Social Security Administration had issued two taxpayers the same SSN.

Standard IRS processes and organizational structure hinder timely and effective case resolution. Demanding telephone schedules, resource restraints, and a large identity-theft inventory make it difficult for assistors to prioritize identity theft cases. Assistors who work the majority of identity-theft cases also work the IRS's toll-free telephones responding to taxpayer inquiries. Identity theft cases are not always priority, even though an untimely case resolution could result in significant taxpayer burden and an improper payment.

Identity-theft case processing is highly decentralized. Coordination among the IRS functions is limited. Procedures pertaining to identity theft are not arranged for efficient access, are inconsistent, and are scattered throughout the Internal Revenue Manual. The different systems used by the various functions prevent accurate tracking and reporting of identity theft workloads and their affect on tax administration. There is no mechanism or system in place to track cases in process or time spent working cases.

[5] Even though a tax return is fraudulent, the IRS retains a record of the tax return by creating a tax account under a tax identification number that the IRS creates, and posting the tax return.

The majority of identity theft cases are worked by telephone assistors. Total time spent on a case can vary significantly and sometimes cases can stay open for months with little or no activity as assistors answer calls or work other types of cases.

Additionally, the management information system that telephone assistors use to control and work cases can add to taxpayer burden. For instance, one victim may have multiple cases opened and multiple assistors working his or her identity theft issue. When victims are asked numerous times to prove their identities, although they had previously followed IRS instructions and sent in Identity Theft Affidavits and copies of identification with their tax returns, this adds to taxpayer burden.

Victims also receive duplicate letters at different times, wasting IRS resources and possibly confusing the victims. None of the letters advise the victims when to expect their refunds, which could still be months away.

Identity theft case histories are so limited that it is extremely difficult to determine what actions have been taken on a case, such as, if research was completed to determine which individual is the legitimate taxpayer. Case histories do not note whether the assistor researched addresses, filing or employment histories, etc., for the individuals associated with the cases. This increases the need to spend extra time on these cases.

When auditors reviewed a sample of cases, they could not determine if some of the cases had been resolved or why the cases were still open. In most cases, TIGTA auditors had to reconstruct the cases to determine if all actions had been appropriately taken to resolve them.

The IRS's standard processes and procedures are not conducive to timely working identity theft cases and need to be streamlined. Victims who contact the IRS when their tax returns are rejected are instructed to mail a paper tax return to an IRS processing site and attach a completed Identity Theft Affidavit along with copies of identification. These tax returns, with the Affidavit and identifying documents attached, are added to the normal processing stream for processing tax returns and casework. They are merely identified as a duplicate tax return and are put in the queue to be worked after the filing season. After the cases are identified as identity theft cases, they then await assignment. This process can take from four to five months.

Transactions to adjust the victims' tax accounts and release the tax refunds can take from 2 to 12 weeks to post, yet the victims may have already received letters advising them that their cases have been resolved. This can lead to additional taxpayer contacts and wasted IRS resources.

The IRS is not able to effectively report on its Identity Theft Program, which inhibits it from taking appropriate actions to reduce identity theft affecting tax administration. The IRS reports cases only for accounts with identity theft indicators.[6] It has procedures in place to input identity theft indicators on certain taxpayer accounts, depending on how the taxpayer's identity theft case was identified and if it affects tax administration. However, the procedures are inconsistent and complex. Potential identity theft cases in process do not have indicators and are not counted. There are approximately 200,000 cases in the Duplicate function inventory that are not being counted. Cases being reviewed, which at any one time can be more than 15,000, may be counted twice. Additionally, identity theft indicators have not been consistently inputted, reversed when necessary, or inputted at all.

The IRS has guidelines to assign temporary Internal Revenue Service Numbers[7] for identity theft cases, but procedures are inconsistent. It does not track or identify which Internal Revenue Service Numbers are created for identity thieves. The IRS also does not classify identity theft cases by employment or refund fraud.

In Fiscal Year 2011, the IRS began issuing Identity Protection Personal Identification Numbers (PIN) to taxpayers who have previously been identified by the IRS as victims of identity theft (when the identity theft affected the filing or processing of their tax return and an identity theft indicator was placed on their account). The PIN will indicate that the taxpayer has previously provided the IRS with information that validates their identity and that the IRS is satisfied that the taxpayer is the valid holder of the SSN. Tax returns that are filed on accounts with an Identity Protection PIN correctly inputted at the time of filing will be processed as the valid tax return using standard processing procedures. A new Identity Protection PIN will be issued each subsequent year in January for the new filing season for as long as the taxpayer remains at risk for identity theft – which depends on whether there are additional fraudulent returns filed using the taxpayer's identity.

Currently, the IRS offers the Identity Protection PIN only to taxpayers who have been a victim of identity theft that has affected the filing or processing of their Federal tax return. It does not offer the Identity Protection PIN to all taxpayers, even if they have reported that they believe they have been a victim of identity theft, but have not had problems filing their tax returns. The financial

---

[6] Identity theft indicators were developed to track identity theft incidents. Each indicator is input as a transaction code with action code and displayed on the affected taxpayer's account. There are various codes that distinguish the type of identity theft incident. For example, a code can indicate (1) the taxpayer identified that they are a victim of identity theft; (2) the IRS identified the taxpayer is a victim and notified the taxpayer; and (3) the taxpayer has submitted the required documentation (Form 14039 and government-issued identification).

[7] This number is created by the IRS for internal processing problems only and is not considered a valid SSN. Tax returns with Internal Revenue Service Numbers are considered invalid by the IRS and as such, the individual is unable to claim personal exemptions, deductions, and credits.

sector offers customers the option of providing additional protection on their accounts. The IRS should consider adopting such practices.

The IRS has an IRS-wide Authentication Strategy, and its goals are to enhance an IRS-wide authentication internal-control framework to address risk, deter fraudulent access, and institutionalize a common set of principles for authenticating taxpayers when contacting the IRS. As the IRS moves forward with this strategy, it should consider controls to prevent fraudulent tax returns from being filed. Providing protection only after the taxpayer has been victimized is a dereliction of its obligation and is not serving the American taxpayer well.

In January 2011, the IRS began working on its latest effort to address the challenges involving identity theft. The Identity Theft Assessment and Action Group was formed in June 2011 to analyze current identity theft operations, identify key pain points and quick actions to improve them, determine a future structure for improving taxpayer service and case resolution, and recommend a plan to achieve these goals. The IRS plans to issue two reports – one on its assessment of the current state of the Identity Theft Program and one on the future state of the program.

**Detection and Prevention of Identity Theft During Tax Return Processing**

A substantial number of unscrupulous taxpayers submit tax returns with false income documents to the IRS for the sole purpose of receiving a fraudulent tax refund from the Federal Government. For Processing Year 2011[8] (through September 10, 2011), the IRS reported that it had identified over 1.6 million tax returns with more than $12 billion claimed in fraudulent tax refunds and it prevented the issuance of more than $11.5 billion (94 percent) of the refunds.[9]

The fraudulent tax returns are identified through the IRS's Electronic Fraud Detection System as well as through the manual screening of paper tax returns. Individual tax returns are sent through the IRS's Electronic Fraud Detection System and are scored based on the characteristics of the tax return and other data. The higher the score, the greater the probability that the tax return is fraudulent. For those tax returns meeting a certain score, the tax return is sent to an IRS employee to screen for fraud potential. If a tax return is selected for further verification, a hold is placed on the tax account for two weeks to prevent the issuance of any tax refund. This delay is to provide IRS tax examiners time to evaluate the tax return for fraud potential, including contacting employers or third parties to verify wage information on the tax return.

[8] A Processing Year is the year that the tax return is processed.
[9] There has been a substantial increase in the number of these fraudulent claims identified. In Processing Year 2008, the IRS identified 381,000 tax returns with $2 billion claimed in fraudulent tax refunds and it prevented the issuance of $1.7 billion of the refunds.

In addition, the tax returns identified included individuals who used another person's identity (name and SSN) to file a fraudulent tax return in an attempt to steal a tax refund. The IRS reported that of the 1.6 million tax returns identified as fraudulent for Processing Year 2011, a total of 851,602 of these tax returns, with $5.8 billion in associated fraudulent tax refunds, involved identity theft. These fraudulent tax returns are part of an extensive tax refund scheme that typically involves the submission of paper tax returns using SSNs from individuals who are unlikely to have to file a tax return. The IRS attempts to identify these tax returns through manual screening when tax returns are received and before the tax return is processed. Our preliminary analysis indicates that this fraud scheme has since expanded to include tax returns submitted through electronic filing.

Overall, the IRS does not know how many identity thieves are filing fraudulent tax returns and how much revenue is being lost. However, there are actions that the IRS can take to improve its identification of fraudulent tax returns. In September 2010, we reported that expanded and expedited access to wage and withholding information would significantly increase the IRS's ability to more efficiently and effectively verify wage and withholding information reported on a tax return at the time the return is processed.[10] The Social Security Act[11] limits the IRS's access to the Department of Health and Human Services national repository of wage and employment information. The data contain quarterly wage information submitted by Federal agencies and State workforce agencies. The law limits the IRS's use of the data solely for purposes of administering the Earned Income Tax Credit, and "verifying a claim with respect to employment in a tax return."[12]

In addition, the IRS has not developed processes to expedite the use of wage and withholding data received from the Social Security Administration. We recommended that the IRS develop a process to expedite the availability of wage and withholding information for use in identifying potentially fraudulent tax returns. IRS management agreed with this recommendation, noting that they continue to take strategic steps to accelerate access to information return data with the goal of refund verification at the time of tax return filing and upfront issue detection. The IRS initiated a pilot project to accelerate its access to Social Security Administration wage data. The IRS is working with the Social Security Administration to analyze the costs and benefits of accelerated transfer, perfection, and integration of Social Security Administration data into IRS systems.

---

[10] TIGTA, Ref. No. 2010-40-129, *Expanded Access to Wage and Withholding Information Can Improve Identification of Fraudulent Tax Returns* (September 2010).
[11] 42 U.S.C. § 653(i)(3).
[12] *Id.*

We are currently evaluating the effectiveness of the IRS's efforts to identify and prevent fraudulent tax returns resulting from identity theft.[13] However, at this point, we are in the early stages of our audit of this area. As part of our assessment, we will identify and quantify potential tax refund losses resulting from identity theft. This will involve researching the characteristics of both the stolen identities used and tax returns filed that were confirmed to be fraudulent. We will apply these characteristics to the population of tax returns filed to identify other potential fraudulent tax returns involving identity theft that were not identified by the IRS and to quantify the associated potential tax refund losses.

We are evaluating tax filing authentication processes and the ability of the IRS to prevent identity thieves from filing fraudulent tax returns. Currently, taxpayers who want to file electronically must select a PIN in order to electronically submit their tax return. In an attempt to authenticate an individual's identity, the IRS requires Personally Identifiable Information to be provided, which can include name, SSN, date of birth, and prior year Adjusted Gross Income, to obtain the PIN necessary to sign their electronic tax return.

In addition, we are assessing the IRS's process to ensure the refund is being deposited in an account that belongs to the taxpayer. In 2008, we reported that the IRS had not developed processes to ensure that more than 61 million Filing Season 2008 tax refunds were deposited to an account in the name of the filer, as required by Federal direct-deposit regulations.[14] Analysis of IRS direct deposit data identified bank accounts receiving multiple (three or more) tax refunds. For Calendar Year 2007, more than 700,000 bank accounts received three or more tax refunds totaling approximately $8.14 billion. Direct deposit, which now includes debit cards, is frequently the payment method used by individuals who attempt to commit filing fraud. Direct deposit provides the ability to receive quickly fraudulent tax refunds without the difficulty of having to negotiate a tax refund paper check.

To improve IRS conformance with direct-deposit regulations and to help minimize fraud, we recommended that the IRS: (1) coordinate with responsible Federal agencies and banking institutions to develop a process to ensure that direct deposit payments are made only to a deposit account held in the name of the recipient; and (2) take action to limit the number of tax refunds being sent to the same account. While such a limit would not ensure that all direct deposits are in the name of the filer, it would help limit deposits going to a single account, which could help reduce fraud. The IRS responded that the Federal direct deposit regulations do not specify that the IRS is responsible for ensuring compliance with these regulations. IRS officials believe that coordinating a

---

[13] TIGTA, Audit No. 201140044, *Efforts to Identify and Prevent Fraudulent Tax Returns Resulting From Identity Theft* (planned report issuance in May 2012).
[14] TIGTA, Ref. No. 2008-40-182, *Processes Are Not Sufficient to Minimize Fraud and Ensure the Accuracy of Tax Refund Direct Deposits* (September 2008).

recommendation of this type is beyond their jurisdiction. The IRS was also concerned about limiting the number of direct deposits to a single account because of situations in which an account is in the name of multiple individuals.

We are also evaluating the effectiveness of identity-theft indicators in identifying potentially fraudulent tax returns for review. In January 2008, the IRS began placing identity theft indicators on taxpayer accounts, which they determined had current or potential identity-theft issues. For these accounts, any incoming tax returns using the taxpayers' SSNs are to be systemically screened using a series of filters in an attempt to distinguish legitimate tax returns from fraudulent returns. If the tax return is deemed to be potentially fraudulent, processing of the tax return is halted and sent to a tax examiner for review. Furthermore, we are assessing whether tax returns with a valid Identity Protection PIN are processed correctly.

**Title 26 United States Code Section 6103**

TIGTA's Office of Investigations has the unique responsibility to conduct investigations that protect the IRS's ability to collect tax revenue. These investigations involve violations of Federal criminal statutes and/or standards of ethical conduct. Regarding the coordination of investigating and prosecuting crimes such as identity theft, the ability for the IRS and TIGTA to disclose tax return and/or return information to other Federal, State, or local law enforcement agencies for use in their investigations is controlled by the provisions of Title 26 United States Code (U.S.C.) Section (§) 6103. More specifically, § 6103 restricts access to, and disclosure of, tax information by providing that returns and return information are confidential and are not subject to disclosure except in limited situations as expressly authorized by the Internal Revenue Code.

Section 6103 protects the following information: (1) returns (*i.e.*, tax or information returns as well as attachments, schedules, or supplements) filed with the Secretary of the Treasury (Secretary) and (2) return information. Return information is defined broadly by § 6103(b)(2) but generally includes any information collected by the Secretary with respect to determining liability under Title 26. For example, return information includes a taxpayer's identity, taxpayer identifying number (*e.g.*, SSN or Employer Identification Number), nature, source or amount of income, payments, deductions, and an investigation into an alleged violation of a Title 26 criminal offense (*e.g.*, filing a fraudulent tax return or false statement under penalty of perjury).

Section 6103 contains a number of provisions that authorize the IRS, on behalf of the Secretary, to disclose returns and return information to a State agency or to a local law enforcement agency. For example, § 6103(i) authorizes, in situations involving imminent danger of death or physical injury, disclosure of returns and return information to a State law enforcement agency. In addition, § 6103(d) authorizes disclosure of returns and return information to a State tax

official or State or local law enforcement agencies for the purpose of enforcing State tax laws. Further, § 6103 authorizes disclosure of return information to State or local child support enforcement agencies to facilitate collection or enforcement of child support obligations upon written request of the agency. Lastly, § 6103(c) contains a consent provision that enables individuals or entities to consent to the disclosure of their return or return information. In addition to the previous examples, several other § 6103 provisions authorize disclosure to a State or local law enforcement agency (*e.g.*, information relating to terrorist activity, alcohol fuel producers, and/or investigative disclosures).

To the extent that the IRS determines that an individual has filed a Federal tax return utilizing the SSN of another individual (*i.e.*, possible tax fraud identity theft), § 6103 protects the confidentiality of the potentially false or fraudulent tax return. The IRS is authorized to release such tax return only as authorized by § 6103. Without the consent of the "taxpayer" (*i.e.*, the individual who filed the potentially false or fraudulent tax return), the IRS is prohibited by § 6103 from disclosing the return for purposes of enabling a State or local investigation and/or prosecution of a State criminal statute involving identity theft.

The IRS's Criminal Investigation Division is responsible for investigating allegations of violation of Federal substantive tax-related statutes, including the filing of a fraudulent tax return (26 U.S.C. § 7207) and fraud and false statements under penalty of perjury (26 U.S.C. § 7206). To the extent that the IRS investigates the alleged crime described above, its investigation of the potential violation of a Title 26 criminal offense is "return information" as that term is defined in § 6103(b)(2) and is subject to the same confidentiality provisions referenced above (*i.e.*, without the consent of the subject of the investigation, the IRS cannot disclose the investigation to a State or local law enforcement agency for investigation and/or prosecution of a State law prohibiting identity theft).

**TIGTA Provides Investigative Oversight of Taxpayer Information**

Under the Internal Revenue Service Restructuring and Reform Act of 1998,[15] TIGTA was created and charged with protecting Federal tax administration. TIGTA carries out this legal mandate by focusing on three core components that expose the IRS to risk: IRS employee integrity; IRS employee and infrastructure security; and external attempts to corrupt tax administration. TIGTA's responsibility is substantially broader than that of most other Offices of Inspector General. While all Offices of Inspector General combat fraud, waste, and abuse, TIGTA is also charged with protecting the integrity of Federal tax administration. A component of protecting Federal tax administration is the investigation of criminal activity as it relates to identity theft and fraud within the tax system. TIGTA's jurisdiction in this area includes the investigation of identity

[15] Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

theft that is committed by an IRS employee, an individual impersonating the IRS (primarily phishing and spam e-mail schemes), and tax preparers who steal a client's tax information and disclose it to others or use it themselves for the purpose of committing the identity theft.

Over the past three years, TIGTA pursued 102 investigations of possible or potential identity theft. I will now provide examples of each of the categories that TIGTA investigates to combat identity theft.

*Employee Integrity*

In order to perform their duties, IRS employees have access to taxpayer information. Identity theft initiated by IRS employees most often occurs as a result of an IRS employee who steals taxpayer information from IRS records. TIGTA investigates the unauthorized access or disclosure of tax information by IRS employees. An example was when an IRS employee accessed the accounts of multiple taxpayers for the purpose of appropriating dependent information which he then sold to others who used such confidential tax information to obtain fraudulent tax refunds.[16]

Another example of IRS employee misconduct as it relates to identity theft is an IRS employee who, while employed as a data entry clerk, stole information of other taxpayers, listed on various IRS forms, including Form 1099-B.[17] This particular form lists a taxpayer's income received and withholdings withheld from interest and dividend earnings. The employee then falsified and forged Forms 1099-B to reflect her own personal information. Using the falsified and forged 1099s as support, the employee then filed her own personal tax return claiming the fraudulent information provided on the forged 1099, specifically, the excessive withholdings to obtain a larger tax refund. The employee filed false tax returns for taxable years 2006, 2007 and 2008, and was able to obtain refunds from the IRS in the amount of $175,143.99. In addition, the employee illegally acquired 68 tax returns of taxpayers, which had been received by the IRS but had not yet been entered into the IRS's computer system. The employee then electronically filed fraudulent tax returns for her benefit using the means of identification of some of these taxpayers. Again, in order to increase the amount of refunds the employee could receive, she filed fraudulent tax returns claiming excessive withholdings from dividends and interest income.[18]

*Phishing*

The increase in electronic tax return filing and the migration of Federal tax administration operations into an electronic environment brings an increase to both internal and external vulnerabilities that can be exploited by criminals. An

[16] N.D. Ga. Indict. filed Feb. 22, 2005.
[17] E.D. Cal. Indict. filed Apr. 14, 2011.
[18] *Id.*

example deals with an individual who participated with others to defraud the IRS and taxpayers by fraudulently obtaining income tax returns before they were filed electronically with the IRS.[19] Without the permission of the taxpayers, this individual and the co-conspirators fraudulently changed the income tax returns in order to redirect the tax refund payments to bank accounts controlled by them. The individual and his co-conspirators engaged in a form of phishing by creating fake websites that misrepresented themselves as accredited and authorized to electronically file Federal tax returns. They advertised these bogus websites on the Internet and electronic mail.[20] The individuals received Federal income tax returns prepared for electronic filing by taxpayers who were misled by the fraudulent websites or electronic mail. In addition, the taxpayers' information was changed so that any refunds issued by the IRS would be sent to bank accounts opened by the individual and his co-conspirators. The investigation into the individual and his co-conspirators had identified 44 phishing websites and a total of 27 different bank accounts, which received diverted tax refunds totaling $647,987.[21] Some of these funds were withdrawn by debit and check cards and by automatic teller machines in the United States and elsewhere.

*Tax Preparers*

An increasing number of taxpayers are turning to tax preparers for assistance in preparing their tax returns. Tax preparers can potentially engage in several types of identity theft schemes. An example involved a man who offered to prepare tax returns for free as a service to the community.[22] He filed over 66 tax returns for persons living in Miami-Dade County, Florida, many of whom were members of two churches. He was not affiliated with any IRS-sponsored programs. He was not a certified public accountant nor did he have any formal accounting or tax preparation training. The scheme involved preparation of returns by inflating the deductions and credits on these returns without the filer's knowledge. He had the IRS send the refund money to bank accounts he controlled. In some instances, the tax filers received an amount that they were expecting, while the tax preparer kept the difference. However, in other circumstances, he kept the entire refund money. In total, the tax filings sought tax refunds over $272,000, in fraudulent tax refunds while depositing $206,000 of this amount into accounts he controlled.[23]

**Conclusion**

Tax fraud perpetrated by identity theft is a growing concern, despite the IRS's efforts to address this serious problem. For Calendar Year 2011, the IRS estimates the number of taxpayers impacted by identity theft – just through the

[19] S.D. Cal. Indict. filed Apr. 16, 2009.
[20] *Id.*
[21] *Id.*
[22] S.D. Fla. Plea Agr. Filed Feb. 27, 2009.
[23] Id.

August timeframe – is more than twice the annual estimate for Calendar Year 2008. Whenever identity theft permits criminals to commit tax fraud, law-abiding taxpayers are too often harmed, both financially and personally. Further, the essential trust and reliability of the Nation's tax administration system is eroded.

It is critical for the IRS to deter and detect identity theft before it occurs within the tax return process. Further, the IRS needs a better process to identify and respond whenever tax fraud occurs as a result of identity theft. While the IRS has undertaken important steps and initiatives to prevent the occurrence of identity theft and associated tax fraud, additional controls could help to minimize or prevent future incidences. TIGTA continues to address this escalating problem through audits and investigations that assist the IRS in its efforts to strengthen critical programs, processes, and controls needed to protect sensitive taxpayer data. Moreover, we believe that the escalating rate of identity theft across the Nation warrants additional safeguards and response capabilities that will enable the IRS to avoid unacceptable future losses due to the consequences of tax fraud perpetrated through identity theft.

Thank you, Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, for the opportunity to address this important topic and to share TIGTA's view of specific efforts by the IRS to combat tax fraud perpetrated by identity theft.

Mr. PLATTS. Thank you, Mr. George. Mr. Cimino.
Mr. CIMINO. Mr. Chairman.

**STATEMENT OF RONALD A. CIMINO**

Mr. CIMINO. Mr. Platts, Ranking Member Towns and members of the subcommittee. Thank you for the opportunity to appear before you this morning to discuss the Department of Justice's efforts to combat tax refund fraud arising from identity theft. The Department greatly appreciates the commitment that the chairman, the subcommittee——

Mr. PLATTS. Please put your microphone on.

Mr. CIMINO [continuing]. And staff have made to highlight the serious crimes of identity theft and fraud.

The Department recognizes the critical need to address this ever-growing problem of identity theft. Combating computer theft, including identity theft, is one of the Department's top priorities as set forth in the current strategic plan.

As the Attorney General has said, our core mission is to pursue justice for criminal acts, and that pursuit includes justice for victims of crime. In criminal matters involving identity theft and Federal tax crimes, the IRS investigates these matters and refers them to the Department.

Thereafter, the Tax Division supervises and directly prosecutes some of these matters. The Tax Division prosecutors work closely with assistant U.S. attorneys across the country to develop and prosecute these tax refund crimes.

As part of that process, Federal prosecutors also ensure that victims' rights are respected. These cases are prosecuted by both the Tax Division prosecutors and assistant U.S. attorneys, either separately or jointly.

This close working relationship enables the Department to share knowledge and leverage our resources in order to combat refund fraud across the country. While each prosecution may only involve the single defendant or small group of defendants, in the majority of cases the number of incidents and victims is significantly greater.

Regardless of the number of victims or the amount of the refund involved, the Department evaluates the merits of each case to determine whether the crime can be proven beyond a reasonable doubt. There are cases in various stages in which the Department is investigating and prosecuting perpetrators of identity theft and tax fraud. As described in my testimony, my written testimony, there are statutory restrictions on my ability to comment on the specific facts of these cases.

However, I can assure the subcommittee that the Department continues to vigorously prosecute these cases to the fullest extent of the law. While prevention and early detection are always the first and best line of defense, the Department recognizes that prosecution is also a critical tool when it comes to combating identity theft and tax fraud.

As Deputy Commissioner Miller has stated in his testimony, the IRS is committed to continuing to look for new and innovative ways to detect and stop identity theft. The Department is also committed to stopping identity theft. Our mission to pursue justice can only

be attained if victims receive justice as well. While the Department will never be able to fully eradicate crimes such as identity theft and tax fraud, our persistence, dedication, and success in prosecuting these cases sends a clear message to those who would engage in such conduct that they will be found accountable for their actions.

I would like to thank you, Mr. Chairman, for the opportunity to appear this morning and I'm happy to take any questions.

Mr. PLATTS. Thanks for your testimony.

[The prepared statement of Mr. Cimino follows:]

**Statement of Ronald A. Cimino**
**Deputy Assistant Attorney General for Criminal Matters**
**Tax Division, U.S. Department Of Justice**
**before the**
**House Oversight and Government Reform Committee**
**Subcommittee on Government Organization, Efficiency and Financial Management**
**Concerning**

**Tax Theft Perpetuated Through Identity Theft**
**November 4, 2011**

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, thank you for the opportunity to appear before you this morning to discuss the Department of Justice's (Department) efforts to combat tax refund fraud arising from identity theft.

The Department greatly appreciates the commitment that the Chairman, the Subcommittee, and staff have made to highlight the serious crimes of identity theft and tax fraud. The Subcommittee's hearings on June 2, 2011, and this hearing today, bring attention to criminal behavior that threatens the fundamental integrity of our tax system. Although we stand ready to enforce the tax laws whenever and wherever necessary, enforcement is only one element of successful tax administration. Thanks to your efforts, taxpayers will have a greater understanding that they need to detect and report identity theft and tax fraud. Those who are engaged in

designing and carrying out these tax fraud schemes will also be on notice that their crimes will be detected and prosecuted to the fullest extent of the law.

In conducting law enforcement investigations, the Department goes to great lengths to ensure that the government's inquiry is complete, and that testimony and evidence are gathered and fully analyzed outside of the public arena. Our policy of not disclosing non-public information about ongoing matters protects the rights of individuals who may be assisting in the investigation, the rights of those under investigation and criminal defendants, and the integrity of the investigation itself. Our ability to comment is also circumscribed by Federal Rule of Criminal Procedure 6(e), which protects the disclosure of grand jury information. In a tax case, the tax privacy statute, 26 U.S.C. § 6103, further limits the government's ability to disclose tax information. Therefore, my remarks today will be limited to information that is already available in the public record.

At some point in our lives too many of us have experienced, or will experience, the stressful moment when we

realize that a credit card or our identification is lost or stolen. If we are fortunate, the only cost we suffer is the inconvenience of obtaining new accounts and identification. However, for victims of identity theft, the economic and personal consequences are much more severe and often long-term. As the victims who testified before the Subcommittee's hearing on June 2 eloquently recounted, in addition to suffering the original theft of their identity, the crime against them was compounded when the stolen information was then used to steal the federal tax refund to which they were legally entitled. Further, when a stolen identity is used to commit tax refund fraud, all Americans are impacted by the loss to the federal fisc.

In recognition of the importance of the problem, the Department and the IRS have devoted significant resources to the successful prosecution of a number of individuals who have engaged in identity theft and tax fraud. While the schemes used to steal identities vary, in many instances the stolen identity was used to access an unwitting victim's legitimate tax refund. Depending on the facts of a particular case, we can bring a variety of charges, including aggravated identity theft, filing a

false claim for refund and conspiracy. While each prosecution may only involve a single defendant or a small group of defendants, in the majority of cases the number of incidents and victims is significantly greater. In the last several years, the Department has successfully prosecuted a variety of cases in which a stolen identity was used to commit tax refund fraud.

Some recent examples include:

- In January 2011, Lester Morrison, a Bronx tax return preparer and leader of a tax fraud scheme that resulted in the issuance of more than $28 million in fraudulent refunds, was sentenced to 72 months in prison. Morrison and his four co-defendants, who also pled guilty, were accused of filing more than 7,500 returns over a ten-year period using, among other deceptive practices, the stolen identities of deceased children.
- In March 2011, Ora Mae Adamson of Montgomery County, Alabama, was sentenced to 46 months in prison for her role in a conspiracy to file 158 false returns using stolen information. One of her co-conspirators, Jeffery Ceaser, was sentenced to 36 months in prison.

- In September 2011, Dalawni Hollomon of Snellville, Georgia was sentenced to 72 months in prison for filing over 700 federal and state tax returns containing stolen information.

Our success in prosecuting these and many other cases is the direct result of the close cooperation among the Tax Division, the United States Attorneys' offices, and the IRS. The Tax Division supervises most federal tax prosecutions. Tax Division prosecutors work closely with IRS Criminal Investigations Special Agents to develop and prosecute a wide array of tax crimes, including tax refund fraud arising from identity theft. Tax Division prosecutors also routinely provide tax expertise to United States Attorneys' offices across the country. These close working relationships enable the Department and the IRS to share knowledge and leverage resources in order to combat refund fraud across the country.

The ability of the IRS to share tax information with the Department and others is governed by 26 U.S.C. § 6103. Section 6103(a) requires officers and employees of the United States to keep tax returns and return information confidential,

and prohibits them from disclosing such information, except as specifically authorized by the Internal Revenue Code. Thus, absent a specific exception, tax information received by the IRS must remain confidential and cannot be disclosed. To the extent that an exception applies and the IRS is able to disclose the information to another officer or employee of the United States, the recipient is also subject to the confidentiality requirements of section 6103. In recognition of the Department's role in prosecuting and litigating tax cases, Congress included specific exceptions to permit the IRS to disclose information to the Department for use by employees who are personally engaged in a proceeding involving tax administration. To safeguard taxpayer privacy, in most instances specific taxpayer information may not be disclosed by the IRS to the Department unless and until a matter is specifically referred to the Department. The successful enforcement efforts I mentioned earlier were possible because of the proper sharing of taxpayer information as authorized by section 6103.

At the Subcommittee hearing in June, the Chairman and the Ranking Member asked how local law enforcement could play a role in investigating and prosecuting identity theft and federal tax refund fraud. Given the unique ability of local law enforcement to understand what is going on in their community, at first glance the idea has obvious appeal. In many instances, the Department has partnered with local law enforcement to successfully combat a wide variety of crimes. For example, in certain cases the Department may formally deputize local law enforcement so they can assist federal law enforcement in a federal tax investigation. However, in these cases local law enforcement is only permitted to access information related to the federal tax investigation, and those who participate in the investigation are not permitted to utilize the tax information in a state or local non-tax investigation or prosecution. While a statutory exception does authorize disclosure to State tax officials and state and local law enforcement who are charged with the administration of State tax laws, this exception would not permit disclosing tax

information to local law enforcement who are pursuing non-tax state charges such as identity theft or fraud.

Since its enactment in 1976, section 6103 has served to protect the personal and financial information provided by American taxpayers to the IRS. The statute plays a critical role in fostering the notion that in exchange for voluntary compliance with their reporting and payment obligations, taxpayers can expect that, absent a specific exception authorizing disclosure, their information will remain confidential. The Department and the IRS go to great lengths to ensure that all of its employees understand and fulfill their obligations to safeguard taxpayer information as required by the Internal Revenue Code.

In crafting limited exceptions to section 6103, Congress sought to balance individual privacy interests with the legitimate needs of tax administration and enforcement. This balance is not an easy one, as clearly demonstrated by the issues that we are discussing today. Given their training and experience in federal tax enforcement, Department prosecutors and IRS investigators are uniquely suited to carrying out the

statutory mandate to strike the proper balance between respecting taxpayer privacy and ensuring compliance with the law. The joint efforts of the Department and the IRS demonstrate that vigorous tax enforcement can be accomplished while respecting taxpayer privacy rights. However, care and consideration should be given to expanding access to taxpayer information to a wide array of agencies and individuals who may not have the same training and experience as federal officials. Expanding the circle too far or too fast might unintentionally erode the safeguards that Congress has enacted in section 6103.

While prevention and early detection are always the first and best line of defense, the Department recognizes that prosecution is also a critical and effective tool when it comes to combating identity theft and tax fraud. It is an unfortunate truth that there will always be a small but persistent segment of society who will seize on any opportunity to make " a quick buck" at the expense of others. While the Department will never be able to fully eradicate crimes such as identity theft and tax fraud, our persistence, dedication, and success in

prosecuting these cases sends a clear message to those who engage in this conduct that they will be held accountable for their actions.

Thank you again, Mr. Chairman, for the opportunity to appear this morning. The Department is interested in properly balancing the privacy interests of taxpayers and the genuine needs of local and state law enforcement. We welcome the opportunity to work with this Committee toward that end. I am happy to take any questions that you or the other Members of the Subcommittee may have.

Mr. PLATTS. Commissioner Miller.

**STATEMENT OF STEVEN T. MILLER**

Mr. MILLER. Good morning, Chairman Platts, Ranking Member Towns, Mr. Nugent, I appreciate the opportunity to speak today.

Over the past few years, the IRS has seen a significant increase in identity theft. Identity theft and the harm that it inflicts is a problem that we are taking very seriously. At the start, let me say quite plainly that the IRS is confronted with the same challenges as every major financial institution in preventing and detecting identity theft.

We cannot stop all identity theft. However, we are better than we were, and we will get better still. We have to balance the need to make payments in a timely manner with the need to ensure that claims are proper and taxpayer rights are protected.

Let me describe our current efforts in terms of fraud prevention first and victim assistance after that. First, up-front protection of fraud. In 2011, the IRS to date has protected $1.3 billion in refunds from being erroneously sent to identity thieves. And for 2012, the following is in place. Despite a very tight budget, we are adding staff in this area.

New for 2012 is up-front screening filters that will improve our ability to spot false returns before a refund is issued. This includes a series of improvements for decedent identity information.

For returns caught in these screens, new procedures are in place. Before any refund, we will correspond with the sender. We are issuing special identification numbers, the PINs, to expedite filing for those taxpayers whose identities have been stolen, and we are accelerating the matching of information returns in order to have a better shot at stopping the fraud up front.

There are new procedures to allow us to match returns to lists of taxpayer information that law enforcement officials believe may have been stolen. We will be doing that up front, and we have improved collaboration with the software developers and others to determine how we can better partner to prevent theft.

In addition, the investigative work done by our Criminal Investigation Division continues, and we will increase the resources available and redouble our efforts to work with other law enforcement in this area. That's our work on prevention.

We are also taking a number of actions to help victims of identity theft. We are implementing new procedures and adding staff to resolve cases faster and minimize the disruption to innocent taxpayers. Newly formed special units will do this work.

The PINs I spoke about earlier will assist the identity theft victims in filing future returns. Next week we begin the process of issuing more than 250,000 such PINs. We have also updated training for our telephone representatives and developed training for all other public-facing employees. Outreach to the public will continue as well.

Let me conclude, our work here is critical. We see identity theft as affecting the way people view our agency and, as importantly, as eroding people's view of their obligation to pay taxes. We cannot be lax in stopping fraud and we must improve our treatment of victims.

I can't tell you that we're going to beat this problem 1 year, but I can say that our work in 2012 is a solid start and not the end of our efforts. And obviously I'll be happy to answer any questions.

Mr. PLATTS. Thank you, Commissioner Miller.

[The prepared statement of Mr. Miller follows:]

**WRITTEN TESTIMONY OF**
**STEVEN T. MILLER**
**DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT**
**INTERNAL REVENUE SERVICE**
**BEFORE THE**
**HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM**
**SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY AND FINANCIAL MANAGEMENT**
**ON IDENTITY THEFT**

**NOVEMBER 4, 2011**

## INTRODUCTION AND SUMMARY

Chairman Platts, Ranking Member Towns and Members of the Subcommittee on Government Organization, Efficiency and Financial Management, my name is Steven Miller and I am Deputy Commissioner for Services and Enforcement at the Internal Revenue Service. I appreciate the opportunity to testify on the important issue of identity theft and provide you with an update on actions that the IRS is taking in this area.

Over the past few years, the IRS has seen a significant increase in refund fraud schemes in general and those involving identity thefts in particular. Identity theft and the harm that it inflicts on innocent taxpayers is a problem that we take very seriously. In his June testimony before this Subcommittee, Commissioner Shulman described the IRS' comprehensive identity theft strategy. It is a two-pronged strategy, focusing both on fraud prevention and victim assistance.

Identity theft is the use of an innocent person's identifying information stolen from a wide variety of places and through a wide variety of means. With respect to the IRS, identity theft manifests itself in several ways. First, it is used to defraud the government of funds through the filing of fraudulent refund claims. Second, it victimizes the innocent taxpayer by impeding his or her ability to get a refund from us. Fraudulent filings may also cause us to initiate an adverse enforcement action against the innocent taxpayer. At the start let me say quite plainly that the IRS is confronted with the same challenges as every major financial institution in preventing and detecting identity theft. The IRS cannot stop all identity theft. However, we are committed to continuing to improve our programs. We can and will work to prevent the issuance of fraudulent refunds and we can and will work with innocent taxpayers to clear their accounts and/or get them their money faster in a courteous and professional manner.

While I will describe for you some of the details of new programs and systems that the IRS has created to address this challenge, I would start by saying that we have put a significant amount of time into redoubling our training efforts for IRS customer service workforce so that they can better understand what identity theft victims are going through. Although these thieves steal the information from sources outside the tax

system, the IRS is sometimes the first to inform the individual that identity theft has occurred.

The IRS has also taken actions to be better prepared in both fraud prevention and victim assistance. On the prevention side, this means implementing new processes for handling returns, new filters to detect fraud, new initiatives to partner with stakeholders and a continued commitment to investigate the criminals who perpetrate these crimes. As for victim assistance, the IRS is working to speed up case resolution, provide more training for our employees who assist victims of identity theft, and step up outreach to and education of taxpayers so they can prevent and resolve tax-related identity theft issues quickly.

The improvements that the IRS is making would not be possible without the additional resources that we have directed toward these programs. We have substantially increased our resources devoted to both prevention and assistance. Even in a declining budget environment, we are hiring and training new staff to address the growing challenge of identity theft.

Fighting identity theft will be an ongoing battle for the IRS, and one where we cannot afford to let up. The identity theft landscape is constantly changing, as identity thieves continue to create new ways of stealing personal information and using it for their gain. We at the IRS must continually review our processes and policies to ensure that we are doing everything possible to minimize the incidence of identity theft and to help those who find themselves victimized by it.

And yet there is a delicate balance here. We cannot manually inspect 100 million refunds to ensure all are correct – nor is there any justification for doing so. That is not practical nor in keeping with Congressional intent. The IRS has a dual mission when it comes to refunds, particularly when they are generated in whole or in part by tax credits. Refundable credits are provided to achieve important policy goals, such as relief from poverty or boosting the economy. The IRS must deliver the promised refunds in the intended time frame, while ensuring that appropriate controls are in place to minimize errors and fraud. We must balance the need to make payments in a timely manner with the need to ensure that claims are proper and taxpayer rights are protected.

So it is indeed a difficult challenge to strike the right balance. The IRS's approach to tackling identity theft must be multi-faceted. We are improving processes to prevent fraudulent filings from being processed as well as identifying promoters and other schemes. We are also taking actions to improve handling of identity theft cases and to better serve taxpayers whose identity has been stolen for tax purposes. Let me walk through our work to prevent the fraud up front and how we hope to improve our service to the victims of identity theft.

**PREVENTING FRAUD FROM IDENTITY THEFT**

Tax filings can be affected by identity theft in various ways. For example, an identity thief steals a legitimate taxpayer's personal information in order to file a fake tax return and attempt to obtain a fraudulent refund. Or, an identity thief may use someone else's name and social security number to obtain a job, which may result in the issuance of a W-2 reporting wage income that ends up being wrongly attributed to the legitimate taxpayer.

Since 2008, the IRS has identified more than 404,000 taxpayers who have been impacted by identity theft. In calendar year 2011 to date, the IRS has protected $1.3 billion in refunds from being erroneously sent to identity thieves. The IRS is committed to improving its approaches to blocking these fraudulent refund claims. To that end, we strive to process returns in such a way that potentially false returns are screened out at the earliest possible stage.

***Catching the Refund At the Door -- Enhanced Return Processing***

Identity theft is a key focus of a new IRS program launched this year. Under this program, a cross-functional group made up of various IRS divisions continues to work to develop enhanced revenue protection processes and policies for the 2012 filing season and beyond. The work being done by this group includes the following:

- Designing various new identity theft screening filters that will improve our ability to spot false returns before they are processed and before a refund is issued. For example, new filters are being designed to flag returns if certain changes in taxpayer circumstances are detected. It must be noted that effective filters are difficult to develop given the number of changes that many taxpayers experience in a year. For example, annually 10 million of us move and 46 million of us change jobs. Thus, changes in taxpayer circumstances do not necessarily indicate identity theft.

- Implementing new procedures for handling returns that we suspect were filed by identity thieves. Once a return has been flagged, we will correspond with the sender before further processing of the return.

- Issuing special identification numbers (Identity Protection Personal Identification Numbers or IP PINs) to taxpayers whose identities are known to have been stolen to facilitate the filing of their returns and prevent others from utilizing their identities. The use of IP PINs is more fully described below.

- Accelerating the availability of information returns in order to identify mismatches earlier, further enhancing our ability to spot fraudulent tax returns before they are processed.

- Developing new mechanisms to stop the growing trend of fraudulent tax returns being filed under deceased taxpayers' identities. First, we added to our process for re-routing returns where it appears that an identity thief has used a decedent's SSN. Second, we will expand on a successful pilot program in 2010 that marks the accounts of deceased taxpayers to prevent misuse by identity thieves. We have marked 230,000 accounts of decedents. This will be an ongoing process. Third, we are working with the Social Security Administration in order to more timely utilize the information SSA makes available to us.

- We have also devised procedures for handling lists of taxpayers' personal information that law enforcement officials discover in the course of investigating identity theft schemes or other criminal activity. This is extremely valuable data that can be used to flag taxpayer accounts and help us block returns filed by identity thieves who have used the personal information of these taxpayers. Our Criminal Investigation (CI) division will utilize this data to ensure linkages are identified between criminal schemes and will also ensure that the information is shared appropriately to affect victim account adjustment and protection activity.

- We have expanded the use of our list of prisoners to better utilize the list to stop problematic returns. We recently received additional help under the United States-Korea Free Trade Agreement Implementation Act that would require federal and state prisons to provide information on the current prison population. We intend to engage with prison officials to determine the best way to move forward with this new authority.

- We are also collaborating with software developers and other industries to determine how we can better partner to prevent theft.

***Stopping It Before It Starts -- Criminal Investigation Work***

The investigative work done by our Criminal Investigation (CI) division is another major component in our effort to combat tax-related identity theft. CI investigates and detects tax fraud and other financial fraud, including fraud related to identity theft, and coordinates with other IRS divisions to ensure that false refunds involving identity theft are addressed quickly and that the IRS accounts of identity theft victims are marked to help prevent any future problems. CI recommends prosecution of refund fraud cases, including cases involving identity theft, to the Department of Justice.

CI works closely with the other IRS divisions to improve processes and procedures related to identity theft refund fraud prevention. For example, CI provides regular updates to the IRS' Wage and Investment division regarding emerging scheme trends so that processes and filters can be enhanced to prevent refund loss. These collaborative efforts have been instrumental in helping the IRS stop more refund fraud.

CI investigations of tax fraud related to identity theft have increased significantly over the past two fiscal years and we expect that will continue in the coming year. In FY 2011, 276 investigations were initiated, compared with 224 in FY 2010 and 187 in FY 2009. CI recommended 218 cases for prosecution in 2011, compared with 147 the previous year and 91 in 2009. Indictments in identity-theft related cases totaled 165 in 2011, with 80 individuals sentenced and average time to be served at 44 months. This compares with 94 indictments, 45 individuals sentenced and a 41-month average sentence in 2010.

This area has been designated as a priority in 2012. We also will be piloting dedicated cross-functional teams with other parts of the IRS that will allow us to create a greater footprint in one or more geographic locales.

Some of the recent successes involving identity theft include the following cases in which sentences were handed down during August-September:

- An Ohio woman was sentenced to 75 months in prison and ordered to pay more than $3 million in restitution after she pleaded guilty to mortgage fraud, tax fraud, credit card fraud and aggravated identity theft. This individual filed approximately 140 false returns using stolen personal information.

- A North Carolina man was sentenced to 132 months in prison, three years of supervised release and ordered to pay $464,000 in restitution on charges that included preparing false tax returns and aggravated identity theft. This individual, who worked for a government agency as a data warehouse manager, was accused of stealing personal information and using the information to file the false returns and make fraudulent refund claims.

- A Georgia woman was sentenced to 72 months in prison, three years of supervised release, and was ordered to pay approximately $290,000 in restitution for filing hundreds of false tax returns using identities stolen from deceased persons.

- A South Carolina woman was sentenced to 37 months in prison, three years of supervised release and ordered to pay more than $125,000 in restitution for making a false claim for a tax refund and for identity theft. This individual received more than $125,000 in false refunds. The false returns she prepared included about a dozen that used identifying information that she had fraudulently obtained.

Local law enforcement and other federal agencies play a critical role in combating identity theft. Thus, an important part of our effort to stop identity thieves involves partnering with law enforcement agencies. We collaborate on these issues and this effort will only increase going forward. It should be noted, that the existing rules for protecting taxpayer privacy often make it difficult for us to provide easy access to information that may be useful for local law enforcement. Nonetheless, CI special

agents throughout the country participate in task forces and working groups with federal, state, and local law enforcement that target tax related identity theft crimes. CI personnel also coordinate with these agencies in an effort to ensure that victims are aware of the steps they need to take to resolve their affected tax accounts. We will continue to develop new partnerships with law enforcement agencies in the 2012 filing season and beyond.

**ASSISTING TAXPAYERS VICTIMIZED BY IDENTITY THEFT**

Along with prevention, the other key component of the IRS' efforts to combat identity theft involves providing assistance to taxpayers whose personal information has been stolen and used by a perpetrator in the tax filing process. This situation is complicated by the fact that identity theft victims' data has already been compromised outside the filing process by the time we detect and stop perpetrators from using their information.

This year, the working group on identity theft reviewed the most effective ways to lessen the impact of identity theft on taxpayers at all stages. As a result of the group's work, we are taking a number of actions, including those described below. As you know from your prior hearings, we have had great difficulty keeping pace with the number of cases. As I mentioned, we can and will do better. We have committed additional resources, even in this tough budget climate, trained our people, developed an IP PIN program, and expanded our external outreach.

***Improving our work on Identity Theft Cases***

As indicated, since 2008, the IRS has identified more than 404,000 taxpayers who were victims of identity theft. We realize the importance of resolving these cases quickly and efficiently, so that identity theft victims who are owed refunds can receive them as soon as possible and so that we do not take adverse enforcement actions against such individuals.

We are implementing new procedures designed to resolve cases faster and minimize the disruption to innocent taxpayers. For example, every division within the IRS will make identity theft cases a higher priority in their work. As indicated above, new procedures and additional staff will be in place in 2012 to work cases faster where a refund has been stopped.

Along with taking steps toward faster resolution of identity theft cases, we are also working on creating a way to timely and accurately track and report on the status of all identity theft cases. By having such a system in place in the upcoming filing season, we believe that the amount of time used to work these cases will decrease, and affected taxpayers will receive their refunds sooner. Additionally, better tracking and reporting means that we can spot – and correct – any flaws in the system more quickly.

***Identity Protection PIN Program***

In addition to helping identity theft victims clear up problems with their IRS accounts, the IRS works proactively to help ensure that these taxpayers do not encounter delays in processing their future returns. In January 2011, we launched a pilot program for Identity Protection Personal Identification Numbers (IP PIN). The IP PIN is a unique identifier that establishes that a particular taxpayer is the rightful filer of the return. Under this pilot, we issued IP PINs to over 50,000 taxpayers who were identity theft victims.

The pilot program showed us that this is a very promising innovation that can dramatically reduce the number of taxpayers caught up in delays. Therefore, we have expanded the program for the new filing season, and will be issuing IP PINs to more than 200,000 taxpayers who have suffered identity theft in the past.

***Employee Training***

The IRS runs one of the largest phone centers in the world, and is dedicated to providing quality service with a high degree of accuracy to every taxpayer who contacts us. Having said that, we realize that taxpayers who call the IRS with identity theft problems present unique challenges to our telephone representatives. Moreover, as indicated in the prior hearing, there may have been instances in which our assistors did not perform as well as we would desire.

Therefore, we recently conducted a thorough review of the training we provide our employees to make sure that they have the tools and sensitivity they need to respond in an appropriate manner to those who have been victimized by identity theft.

As a result of this review, we have done two things:

- First, we updated the training course for our telephone representatives in order to ensure that our assistors maintain the proper level of sensitivity when dealing with identity theft victims and understand the serious financial problems that identity theft poses for these taxpayers. This training will be provided in advance of the 2012 filing season.

- Second, we broadened the scope of our training to cover those IRS employees who are not telephone assistors but who nonetheless interact with taxpayers or work identity theft cases. We have developed a new course for these employees, which will include not only sensitivity training but will also ensure that employees who process identity theft cases have the proper tools and techniques to do so. This will be provided to selected employees during calendar year 2012.

***Taxpayer Outreach and Education***

The IRS continues to undertake outreach initiatives to provide taxpayers, return preparers and other stakeholders with the information they need to prevent tax-related identity theft and, when identity theft does occur, to resolve issues as quickly and efficiently as possible. Recent actions in this area include the following:

- We overhauled the identity protection training provided to tax practitioners at this year's Tax Forums. These yearly events, held in several cities around the country, typically draw more than 16,000 practitioners. In addition, our Small Business/Self Employed division held a meeting in October with practitioners that included a discussion of the IP PIN program, the expansion of the program, and the modified procedures, forms and notices associated with the program.

- We continue to update the identity theft information provided on the IRS.gov website. This includes emerging trends in identity theft along with fraud schemes, phishing sites and prevention strategies. We recently added a direct link to our Identity Theft page, to make it easier for taxpayers who visit IRS.gov to find it.

- We produced two new identity theft awareness videos for our YouTube channel, and will be communicating various identity protection messages via Twitter. We plan to continue producing YouTube videos on identity theft and communicating via Twitter about this issue throughout the upcoming filing season.

**CONCLUSION**

Mr. Chairman, thank you again for the opportunity to appear before the Subcommittee and update you on the steps that the IRS is taking to prevent identity theft and to assist taxpayers who have been victims of this crime. This work is a key challenge for the IRS at this time. We see it as affecting the way people view our agency and, as importantly, as eroding peoples' view of their obligation to pay taxes. Our work here for filing season 2012 is a solid start but not the end of our efforts. I cannot tell you that we will beat this problem in one year. I can tell you that we have committed our talents and resources to prevent the issuance of fraudulent refunds and have developed processes to minimize the pain felt by those who have been victimized. We are committed to continuing to look for new and innovative ways to improve our processes and techniques. I would be happy to answer any questions that you may have about our role in guarding against identity theft and assisting its victims.

Mr. PLATTS. I yield myself 5 minutes to begin the questioning and again thank each of you for your testimony as we work jointly to try to address this growing problem and better protect American taxpayers and to prevent American citizens from being victimized.

And I want to start with the issue of how we are assisting victims. And, Commissioner Miller, you and I have spoken about this issue prior to this hearing as we did with the Commissioner back in June, that we recognize we're talking about criminal acts here and the victims of crime.

And I'd be interested I guess first, your response both here today and in the written testimony of the Inspector General, when they look at a typical way that a victim of identity theft within IRS has been handled, where they first learn of it in February, report it, and then work their way through the Inspector General kind of references, what they see based on their findings, a typical case where you know they—the law-abiding citizen, when they go to file their return in February and finds out somebody has already filed a return under their name and Social Security number—that they work through February, April, July, September, October November, December and January as a typical response till that person's case is resolved.

And my understanding of the standard procedure is that when one of these cases come to light in February or March, that is basically put into what's called a duplicate case filing system and basically set aside until, at the earliest, sometime after April 15th when the filing deadline hits.

That's not giving much priority to the victims of crime, which is what we're talking about here.

So I guess, Mr. Miller, your response of how you assess the Inspector General's review and, you know, what we are doing to change that, because that's not an acceptable level of response.

Mr. MILLER. And I agree with the presentation that you have just given. Let me break this up into about three pieces. First, as to Mr. Russell's report, we have not seen his actual report. The first we saw it was Wednesday night so it's hard for us to exactly judge and deal with point by point.

But I will say, not our understanding, and we don't think it's correct that the typical case—whereas as he used in his written testimony, the best case is 18 months, we don't think that's right. We're going to go back and we'll take a look. But, you know, I am also going to say I'm quite sure it has happened, right? I don't think it's typical. I know it's happened.

Mr. PLATTS. When you take that look, if you could submit to the committee for the record what you find is the typical average response from the time that person says I've been that victim and their case is resolved.

Mr. MILLER. Be more than happy to do that.

[The information referred to follows:]

[NOTE.—The information referred to was not provided.]

Mr. MILLER. The second piece that you talked about is is this a priority for the service, and it's a tough answer. The answer is that when it happens early in the year, that's when the same people who are doing this work are doing phone work.

Is it a priority, is it a first priority? Yes. But the question is, are we going to do phone work or are we going to do these cases? We need to do a better job going forward of doing both. That's a resource issue for us, to be blunt.

I think, I think probably in 2011 we did more phone and less paper. I believe for 2012 with the resources that I've made available we'll do more paper. There's still going to be resource shortages. And while we will try to get to this work, there's an awful lot of work that goes on during that timeframe. We need to process returns.

We need to, you know, deposit checks. We need to answer the phones. And our phone level of service is not something to wave the flag about either at this point due to resources. We're down to, you know, 7 out of 10 people getting through. And next year, you know—this year, rather, in 2012, it's likely to go down from that. So we have some tough choices to make up front. But I will tell you we're going to do better this year. We've made more resources available to work both of these things.

The final piece, and that really is the final piece, the final piece is we are going to get better at this. And we are putting in place units, specialized units in accounts management, in submission processing, in the other places where identity theft presents itself, in order to work these cases quicker, to work them with folks that understand the processes better. They will be trained; we will do a better job this year.

Mr. PLATTS. And you reference in your testimony the training that you're doing, which clearly is necessary.

Mr. MILLER. Right, it is.

Mr. PLATTS. But it's also an organizational challenge because I think you identified, what the Inspector General identified, is that you have the individuals that are on the front lines of the phones also being the one charged with assisting victims. And so to meet the needs of the phone calls, you're in essence setting the victims assistance aside—as the Inspector General referenced, the duplicate function—so that it's treated as just a duplicate case and not given a priority.

And I guess as I've shared with you previously and again today, when it comes to a victim of a crime, we need to make that a priority.

Mr. MILLER. I understand.

Mr. PLATTS. And I don't think we're adequately doing that. I think you understand the importance of that and the training that you're doing. I commend you for that approach and—but I think it is an organizational structural issue here that you need to, you know, have a victims assistance unit that is not worried about meeting their other obligations over here but is focused specifically.

These are law-abiding citizens who are trying to comply with, as we all know, a very complex code. We bear the blame here in Congress for that, but they're trying to do their part, and then they get victimized and we need to do a better job of assisting them.

And a quick follow-up, and then I'll yield to the ranking member. I know I'm over my time.

But if you assume that you were even close in the Inspector General's findings, it's identified in February and it's the following Jan-

uary or so until it's resolved, in this written testimony there's also statements that they found that even when the victim of the crime is being given notice that your case is resolved, you're good, that it's anywhere from 2 or more weeks till the payment, the refund, is actually provided. So, you know, what's the delay there?

You've gone through 10, 11 months. They get a letter saying, yep, we understand. We've gotten it straightened out, but they still wait, you know—you know—in the statement it says release of tax refunds can take from 2 to 12 weeks to post. That's pretty outrageous, you know, that it's done but it still takes us up to 3 months. So I don't know if that's an issue that you've looked at yet, but we need to.

Mr. MILLER. So I can come back with more information on that, Mr. Chairman. But in my understanding it will take 2 weeks, probably, because we work in cycles. It might take, depending on when it occurs in that 2 weeks, 4 weeks, never really should take 12 weeks, and I need to take a look at what TIGTA is looking at to work through that.

Mr. PLATTS. Right. But in your response there, I would emphasize again, we need to prioritize assistance to the victims, to not put them in the normal cycle. We're going to issue checks in 2 weeks or 4 weeks or 6 weeks. Now these guys have waited 11 months after being victimized. So I think we—what I hope you'll look at is how do we prioritize these, not just put them in the normal routine standard operating procedure. But, no, they have already, you know, waited long enough to simply get what they are owed, in essence, by us.

So I appreciate you taking those concerns back and understand that you—I do not expect to have all the answers here today, but that we—we are on the same page as far as trying to do right by the victims.

With that I yield to the ranking member, Mr. Towns, for the purpose of questions.

Mr. TOWNS. Thank you very much, Mr. Chairman.

Let me begin with you, Mr. Cimino. How many attorneys currently work on tax fraud issues in the Department of Justice across the United States?

Mr. CIMINO. Congressman Towns, I can't—I can't respond the number across the country, and I can get back with you with a little more detailed information, but I can try to respond to your question.

Within the Tax Division we have 100 or more prosecutors solely devoted to tax fraud. Most of those positions are filled by line attorneys who have two roles. One is to ensure that the investigation that the Internal Revenue Service has conducted and submitted to us is adequate for a successful prosecution.

And the second role is to actually prosecute those cases across the country. We do that ourselves. We do that cooperatively with the U.S. attorney's offices as co-counsel with them, and a great bulk of the cases are actually handled by the 94 U.S. attorney's offices' staff across the country.

Each year there's a certain number of cases forwarded to us by the IRS, and we try to process them as quickly as we can to move them on.

I hope that answers your question, sir.

Mr. TOWNS. Well, I guess you answered my question but I guess what I'm really thinking about is, isn't it time for you to start partnering with local law enforcement? Don't you think we should do more of that?

Mr. CIMINO. In response to your question, we——

Mr. TOWNS. I'm aware of section 6103.

Mr. CIMINO. We do, in fact, have joint task forces with local and State law enforcement working with task forces in the various U.S. attorneys's offices. The State and local officials are deputized under the U.S. Marshals program and work in a cooperative spirit. This usually occurs in a grand jury setting.

Mr. TOWNS. Let me ask you, do you have any information on them, the conviction rate—in terms of the actual conviction rate?

Mr. CIMINO. In terms of all cases across the country that are tax-related historically, and I have been with the Department since 1973, it has always been higher than 90 percent; frequently 95, 96 or 97 percent of a conviction rate for the charges of the crime.

Mr. TOWNS. You know, if you think that if we partnered more with local law enforcement the number would go down—do you think that would happen if we partnered more with local law enforcement, would the number go down? Do you think that; or would it remain basically the same?

Mr. CIMINO. I can't, could not venture. I'm sure that our local and State law enforcement are very effective prosecutors.

The problem, perhaps, Congressman, is that in partnering we have to be prosecuting Federal crimes, and in that sense my answer to you is no. I think almost every U.S. attorney welcomes the assistance of those people who are deputized to work in Federal task forces.

Mr. TOWNS. Let me just go to you, Mr. Miller. You indicated that you think you would be able to do a whole lot better. You know, are you getting additional resources?

Mr. MILLER. No, sir. We have had to obviously carve out another 400 or so people to make a dent in this work, which is almost doubling the footprint that we have in this area for identity theft.

Mr. TOWNS. You know, I'm concerned that, you know, when you take from somewhere else, that something else happens.

Mr. MILLER. Yes, sir.

Mr. TOWNS. You know, and that's my concern. So it seems to me that we need to take a serious look and evaluate, maybe, and listen to the testimony from Representative Nugent. Maybe we need to increase the amount, you know, of investigators to be able to—and we might be able to close part of the deficit. Because I'm certain that if you would analyze, and bringing more people on, and then going out and dealing with fraud and abuse, I think that, who knows, that we might make a profit. It might be an increase.

So I think that we need to look at the possibility of getting more workers to stop what's going on because it seems to me that they are under the impression that it's okay. Because when you look at the fact that in 2008, 51,000 cases, and in 2009, 169,000 cases, and in 2010, 248,000 cases, and then in 2011 582,000 cases, and who knows what's going to be in 1912 and 1913.

Mr. CONNOLLY. Would my colleague yield for an observation?

Mr. TOWNS. I would be delighted to.

Mr. CONNOLLY. I couldn't agree with him more. Sadly, this committee is headed in exactly the opposite direction. We approved legislation yesterday that would guarantee at least a 10 percent reduction in this agency and all Federal agencies.

Mr. TOWNS. Well, you know what they say in my neighborhood back in Brooklyn, New York, "We'll hustle it backward."

Mr. Chairman, you know, I think that—I know my time has expired, so I'll yield back.

Mr. PLATTS. I thank the gentleman. And before I yield to Mr. Nugent, I do appreciate the concern expressed about legislation we moved yesterday, but I would emphasize that it's a 10 percent reduction overall. And as we kind of just debated in committee yesterday, meaning that we as a Congress and the Federal Government needs to better prioritize, you know, what are our most important responsibilities. So it doesn't mean that this agency would go down by 10 percent. Maybe it's other agencies that are less important or less important assignments.

So, overall employment would be 10 percent.

Mr. TOWNS. I think——

Mr. PLATTS. I would yield.

Mr. TOWNS. Mr. Chairman, undoubtedly you yield. Thank you. I appreciate it. For a moment I thought I was chairman.

Mr. PLATTS. And the distinguished gentleman has been chairman in the past, as have I. We keep swapping chairs.

Mr. TOWNS. Hold that thought. No, I would just say it seems to me that we need to look at the possibility that bringing in additional revenue is important, and maybe this is an agency that should be increased. I mean, I think that's the point I'm making and that if we increased it, who knows, because I think that is one other thing that we're not examining here.

Some folks that are victims do not even report it. Because when I look at them taking people from another place, then the phone center, I mean people will then—can't get through, they can't make—I mean, I'm concerned about that.

And then there's the other issue of how many people are just ripped off and don't even report it, don't even talk about it because of the fact that it's difficult to be able to get through to the center. So there are those kinds of things.

I yield back, Mr. Chairman.

Mr. PLATTS. Reclaiming my time. And Mr. Towns references a very important issue. We know that many of those whose identities are stolen are individuals who would not need to file a return. And so they, you know, don't know that a fraud's been committed against them because they would not have otherwise filed one. So the actual number of fraud cases, because those individuals don't even know it, are not able to help identify it and allow us to then prosecute the wrongdoer.

We do have votes up on the floor. My intent here is to get to Mr. Nugent's questions and then Mr. Connolly, and then we will have to take a brief recess, shoot over for votes, come back and try not to have you waiting here any longer than you have to.

So, Mr. Nugent, you are recognized for 5 minutes for questions.

Mr. CONNOLLY. Mr. Chairman, just on that, I'm probably going to go and vote. So we'll reconvene after votes?

Mr. PLATTS. We will.

Mr. CONNOLLY. Cool.

Mr. NUGENT. Thank you, Mr. Chairman and the members of the panel for being here today. You know, as a local law enforcement official for so many years, we worked hand in hand a lot of times with the U.S. attorney's office in adopting cases that we worked, that turned out to be federally prosecutable, and we would partner with DEA, FBI, ICE, to bring that forward to the U.S. attorney's office.

And the difference in this scenario, though, is working with the IRS. And it seems like we're—you know, when you talk about leveraging resources, particularly where everybody, everybody is cutting back, I think we're missing the boat as it relates to tapping into that local law enforcement.

Just as in the city of Tampa—you know, not all the crooks live in Tampa, and they're accounting for, you know, millions and billions of dollars in tax fraud alone. And this is real tax dollars, dollars that are already in the Treasury that are now flowing back out.

So my question is, if you understand the code and understand the U.S. regulation, is there a way to better partner with more eyes on the ground to help you enforce? And I would submit that to Mr. Cimino or Mr. George.

Mr. GEORGE. Why don't I start? The IRS has limitations placed on it, as you made reference to, under the U.S. Code, specifically title 26, section 6103, which severely limits the type of information that the IRS can share.

Now, while it limits it, it doesn't restrict it. There are certain circumstances, if someone's life is at threat or there are other exigent circumstances, you know, with the permission of the Department of Justice, the IRS can get permission to work with State and local officials. But sometimes that is a very cumbersome process. Sometimes it really, as you acknowledge here in the Tampa instance, it just would be so cumbersome that it just needs to be looked at closely, I think. And that is, again, section 6103 needs to be looked at by Congress in terms of whether 25, 30 years after Watergate, when most of these restrictions were put up, whether those same restrictions are necessary today.

Mr. NUGENT. And particularly with, you know, the advent of the Internet, because we're looking at mostly filings that police law enforcement has coming across, you know, the e-filings and the ability to raid the Treasury.

Mr. Cimino.

Mr. CIMINO. I agree with you, I think there can be more cooperation, Congressman.

Mr. TOWNS. Microphone, Mr. Cimino. Will you turn your mike on.

Mr. CIMINO. As I mentioned in response to an earlier question, there is a procedure in place when there are Federal grand juries involving widespread crime that local law enforcement are deputized to work in the grand jury under the direction and aegis of the

U.S. attorney, but that is for Federal crimes and we certainly can explore whether that can be used more effectively in this area.

Mr. NUGENT. Mr. George, you had mentioned that in looking at the legislation to, I guess, to more massage that while respecting taxpayer privacy, which is a huge concern for all of us, but at the same time protecting the U.S. Treasury from being raided. So you asked, or what you're saying is that we absolutely need to look at how we can do, through legislation, help from a law enforcement perspective to Mr. Cimino and the U.S. attorney in the Tax Division.

Mr. GEORGE. Yes. And I should have actually, Mr. Nugent, prefaced my earlier response by pointing out that the Secretary of the Treasury has delegated tax policy to the Office of Tax Policy, so I am not speaking on behalf of the Department in terms of advocating, you know, substantive tax policy changes in this area.

But the ironic part about 6103 is that even the alleged cheater can be protected, because the IRS is unable to share, unless certain circumstances exist, information about that person's tax return.

So if you have two competing taxpayers, in the instance we're discussing here, someone who has taken the persona of another person, you know, until the IRS figures things out, their hands are tied in many respects unless someone consents—the taxpayer can always consent to the release of his or her information. But there—this is a very cumbersome area, as I said before, and it needs to be looked at again.

Mr. NUGENT. And one last, just to follow up. As it relates to the front end of this, obviously if you can shut the spigot off it would obviously then, you know, reduce the burden on investigators, reduce the burden on the U.S. attorney's office and the courts. So I would suggest to you that we need to do more specifically as it relates to shutting the spigot off in regards to trying to—you know, we push out the returns as quickly as possible.

But by the same token as the chair had mentioned, once it's identified, the real taxpayer trying to get his return is through a laborious process to get there. So I would suggest or recommend that the IRS really come back with a plan to Congress and particularly to this committee as to how you're going to do that.

Thank you, Mr. Chair. I yield back.

Mr. PLATTS. The gentleman yields back. We're going to try to get a few more questions in before running over for the votes. I think, Mr. Towns, you're going to head over.

Mr. TOWNS. Yes.

Mr. PLATTS. I'll take another round, and then I know Mr. Connolly is coming back and Mr. Towns.

I want to follow up, Mr. George, when you were just talking about the challenges that Mr. Nugent raised, and as you referenced, that even the perpetrator of the crime then has to give permission for anything related to their conduct in committing that crime is still protected.

Is that a possible amendment to the existing law where, you know, we're balancing privacy issues here? But once the IRS is able to certify, yes, this person, the lawful citizen who finds out in February, hey, somebody already filed. They come in, they present all the documentation, Social Security card, other ID, whatever they

need to do in the affidavit, establishing that I am the legitimate John Smith. And that has been established and the IRS is able to confirm that and certify that yes, you are, that would then trigger within the law that the information of the perpetrator of the identity theft is no longer protected and does not have to give permission.

Is that a way of trying to get to the issue, you know, where that—the information could be shared to make it easier to prosecute?

Mr. GEORGE. The short answer is yes, once this process is played out. But it's during the course of it that it's really, you know, sometimes really nonsensical or counterintuitive.

Mr. PLATTS. And it would need, as we talked earlier, Commissioner, to really expedite that process of who is, you know, the lawful taxpayer here, the sooner the better as far as then trying to go after the wrongdoer.

Mr. GEORGE. But that ties into the overall complexity of the process that you made reference to when you were addressing Mr. Miller earlier. There's no question that it's very complex and cumbersome for the average taxpayer in this predicament to get this matter to the point where that determination is made. And so the IRS, they literally have about 16 different divisions within them that handle these types of cases and these types of allegations.

They need a more unified process in place to do this more efficiently and effectively.

Mr. PLATTS. And that goes to Commissioner Miller, the issue, the structure, the organizational structure that, in prioritizing assistance to the victims, that if we do that better and centralize that, we also then maybe help centralize this whole matter, you know, challenge so that we can better go after, you know, the perpetrator of the crimes.

Mr. PLATTS. The issue of prosecution—and Mr. Nugent shared the amazing story of Tampa and the $100 million plus, you know, the dollar amounts, but my understanding is the average tax fraud is about $3,400.

I guess, Mr. Cimino and Mr. George, on your understanding, or maybe specifically from Department of Justice in pursuing—we understand you are looking at those cases where it is $5 million, or $10 million or $100 million—what is the likelihood of that person who files five cases averaging $3,500 of the Department of Justice saying we're going to go after them as well?

Mr. CIMINO. Chairman Platts, there's no one factor that goes into the prosecutorial decision of whether we will or will not prosecute.

We look to all factors and I can assure you if, even if there were a single false return, if the circumstances justify it, we would look at it to see if it warranted prosecution.

Mr. PLATTS. Mr. George, do the numbers show that, that we are prosecuting, you know, those. Because the way, the way I read all the testimony in our June hearing that, you know, if it's $3,400 or $4,000, $5,000, the reality is we don't go after those, and the bad guys know that. So they feel free to continue to engage in this unlawful conduct because they know we're not going to pursue it.

Mr. George.

Mr. GEORGE. You know, while I am not the Inspector General of the Department of Justice, anecdotally, not only in the text context, it's just overall, DOJ has to make choices because of the limited resources that they have. And I'm not in a position to say what the threshold is for prosecuting particular cases. Mr. Cimino may be in a position to respond to that. There's no question that the lower the dollar amount, the less likely they're going to expend a lot of resources.

Mr. PLATTS. And that's my understanding of the data as well.

Mr. CIMINO. If I can further respond, Congressman Platts. Almost all cases that we see at the Tax Division that the IRS has investigated have multiple claims for refund and frequently multiple defendants acting in a conspiracy.

I think the three cases that I included in my testimony, those that were Mr. Miller's, and probably across every U.S. attorney's Web page reflects that and, you know, there's the reality of our work. What I was trying to respond to, is there a situation where a small dollar case would be prosecuted? And that's what I was trying to refer to.

Mr. PLATTS. Yes. And this one really goes to Mr. Nugent, about partnering in the law enforcement community and finding a way to allow that partnering, and I would say incentivize it maybe it's where—I know we do it in some areas of prosecution of drug cases where there's a financial incentive, you know, for the locals to partner with the Federal officials in the recovery of the dollars, and maybe that's the way to do it.

Commissioner Miller, the cases that go to Justice really have to first be identified by IRS saying we want Justice to help. Your Criminal Investigation Division really makes that first determination. Is that really accurate?

Mr. MILLER. I think it is, I think it is. But there are constant conversations going on between the Department of Justice and the IRS about what we—what we would do.

If I could, if I could, Mr. Nugent, we do partner with locals. What happened in Tampa is what happened in Tampa.

But I will say we have more than 20 task forces going on as we speak today. We have 32 investigations in Tampa, and we have spent in 2011, 225,000-plus hours on identity theft.

So I don't want, I don't want the committee to think that we're doing nothing here. We really are. We might have had a foot fault in Tampa, admittedly, and we are doing better in Tampa and we are taking steps to get better in Tampa. We're also taking steps to get better on the front end. With the type of things that we saw in Tampa, I hope won't happen in 2012 with what we put in place.

Mr. PLATTS. That might be a good place to break.

Mr. Nugent, did you have another comment.

Mr. NUGENT. Well, just to go back to that, and let me set the record straight as it relates to the IRS agents, criminal investigators in Tampa, nothing but the highest praise for the individual investigators.

The problem came in regards to when Tampa identified specific cases, that that's where it broke down. And the ability that Mr. George talked about in trying to prosecute cases to—particularly when they identify not only those that, you know, profit from it,

but also where they were money-laundering the cards and the T checks directly, and that's where they ran into a brick wall.

And the frustration on the local law enforcement level is that while we work really well with the U.S. attorney's office and other portions of Justice, that's just not the case as it relates to IRS, not the agents in the field but the bureaucracy that they're working under. And so as times change, that's why I think we're having these hearings, that we've got to get past how we used to do it and figure out how we're going to do it, particularly with the advent of computers. And we watch the bad guys; they morph faster than we can.

Mr. MILLER. Agreed.

Mr. NUGENT. And so I think that's where we need to move forward as a committee but also as a Congress.

Mr. PLATTS. Certainly, Mr. Nugent, I look forward to working with you on the issue of what legislative changes we need to look at and giving more authority and power.

Mr. NUGENT. Thank you for allowing me to sit up on the dais with you and allowing me to testify in front of you.

Mr. PLATTS. Well, we're glad to have you and, again, your knowledge as it relates to your district really gives us a good working knowledge of how to better protect what happened in Tampa not happening again. And, again, we do look forward to working with you.

We are going to recess to the call of the chair. We've got two votes, so hopefully we'll be over and back in about 10 to 15 minutes max. We are going to be limited, you know, when we come back again, but we'll try to wrap up in that next session because there will be another round, actually several rounds, and we don't want you sitting all day waiting for us.

But I know Mr. Connolly is coming back, Mr. Towns. I know when I come back to get to a little bit what we started on, which is the preventive efforts up front, so we don't have to worry about assisting victims if we can prevent them from being victims. And so I think that's where we will pick up when we come back.

So this hearing stands adjourned—I'm sorry, recessed to the call of the chair.

[Recess.]

Mr. PLATTS. The hearing stands reconvened. I appreciate our witnesses and everyone's patience while we—got my exercise for the day running over and back.

So as I referenced before we recessed, I want to get into some of the efforts of prevention. And, Commissioner Miller, one of those issues is—regards the issue of e-filing and the impact that it's had in a wonderful way as one who does e-file myself, that expedited refund process. And I think most Americans are glad to get their money back that they're entitled to as quickly as possible, but it also seems to correlate with the numbers that we see in increased level of fraud, if you'll look at the kind of timing of e-file and it's has been promoted in greater and greater fashion, and then the fraudulent case numbers.

And in the Inspector General's testimony there's reference to what you have to do to be able to e-file and reference to the infor-

mation that has to be provided, and one of those issues was your prior year's adjusted gross income.

And, Commissioner if you could address that issue. What actually is required to e-file besides name and Social Security number, if anything, and, you know, why don't we require additional information to make sure we're guarding against fraud?

Mr. MILLER. So we do, as you mentioned, Mr. Chairman, we do require sort of an electronic signature, and that requires you to have your adjusted gross income from the last year as one of the items. And there are a handful of other items. But it is name, Social and the AGI is that—is one of the shared secrets, along with filing status for last year, I believe. There may be one other that I can get back to you on, but those are the types of things we use today as the electronic signature for the electronic—and a natural question that you raised in our prior discussion was why shouldn't we make that more generally applicable and why doesn't that work to block much of this?

And it does work, I'm quite sure, in many areas. Where it would not work is where there's been no filing requirement in the prior year because there the AGI is zero. And so that is an easy way to go through that system and sign and move through. And we should work, as we've talked about, we should work to see what we can do better in those circumstances.

Mr. PLATTS. And you touch on the one issue, which is the fraud that's committed against those who don't have to file because their AGI is beneath the threshold, and so they only know they are victims of identity theft in—regarding tax fraud.

Is the AGI required for every electronic filing?

Mr. MILLER. I believe it's the manner of how to—how to sign your return. There is—if you have forgotten it, if you don't have it—there's an alternative method to get a different PIN. And if I'm wrong on that, Mr. Chairman, I will come back to you. But there is an alternative if you don't have your AGI. There is a PIN, a way to go online and get a PIN with some shared secrets there as well.

Mr. PLATTS. And, Mr. George, is that what you're referencing in your testimony, because you say, "which can include names, Social Security number, date of birth, prior year's adjusted gross income."

Mr. GEORGE. That's correct. Mr. Miller is correct. There is that alternative way in the event you don't have your AGI.

Mr. PLATTS. So can you walk me through the specifics of what the alternative is, because to me if you have to have your adjusted gross income from the prior year, that's a reasonable requirement to file. And if we're going to make, you know, an alternative to that, I guess I'm not aware of what that alternative process is.

Mr. MILLER. So my understanding, Mr. Chairman, is that you can go online and you would basically have many of those same things, which is name, address, Social Security number, I believe filing status and, again, date of birth as well. And you can get a PIN mailed to you, and that's the process right now. And we ought to look at it to see whether it's everything it ought to be.

Mr. PLATTS. I'd be concerned, if you can follow up with the committee, what the specific requirements are for that alternative electronic signature. Because if it is basically the same information that you have to provide anyways—name, Social Security, date of

birth, not something additional—it's adding a step that you go through something.

But, you know, hopefully there is additional information and I'm not sure if it's, you know, logical that we want to allow to file electronically if you can't document—and if it's zero—zero because you didn't file the previous year, but as a way—what I'm looking for is what are some filters up front to knock out the ability, you know, for these individuals to file electronically.

And a follow-on to this is my understanding is well over half the ID theft, fraud cases, are in January in a typical year; am I correct in that understanding?

Mr. MILLER. I would have to go back and verify that. I think it's front-loaded but I don't know that it's half. It is occurring throughout the year at this point.

I was just informed by staff that your statement is accurate, Mr. Platts, mostly January.

Mr. PLATTS. And, again, my review of the data—and I don't have all the information that the IRS itself has, but is that more than half are in January. And I think there's a reason for that. The perpetrators of the crime know they won't get their W–2s until the end of the month, or even the first week of February, so they're getting their return in first before the lawful citizen.

So that gets to kind of the follow-on, in addition to the adjusted gross income, that my hope is that the IRS is looking at how to further or enhance your scrutiny the earlier return is submitted.

Mr. MILLER. We are trying to move up our review of information returns we're getting, including the W–2. And we're putting in place some filters to try to drop out more returns that look like they are identity theft.

Mr. PLATTS. And I appreciate the sensitivity of what your filters are. We don't want to talk about that here in open—if that can be provided to the committee.

Mr. MILLER. Happy to do that.

[The information referred to follows:]

[NOTE.—The information referred to was not provided.]

Mr. PLATTS. Because looking at the W–2s, if it's fraudulent, you're not going to get any. So expediting that review is not going to help because the criminal is not going to send you any W–2s because they don't have them. So the more—the tighter your filters are and the more kind of flags that go up, new address, new bank account, those types of things.

Can we also talk about, then, the IG's testimony. There was the issue about Social Security death index and a better use of that. And is there additional statutory authority that the IRS needs to better access that information, or it's just how you're currently accessing it to guard against deceased individuals being used, names and IDs of deceased individuals being used to file current returns?

Mr. MILLER. So we have a new sort of approach to deceased identities, and we have locked a bunch of accounts at this point and, again, we'll go into much more detail. But in general we have locked a great number of accounts that don't have a filing status, we believe.

There were some decedents who have a filing status there, in 2010 and 2011, for example, they would have a filing, a last return.

And those we've built new filters to take a look at up front and intend to take a hard view on.

The Social Security list of those who have passed, it is an issue for us. We are getting it, we are matching it and we'll do a better job of that going forward. Ultimately we would, you know, we would love if Social Security did not—or had a different manner of posting it, but they are constrained by law and by lawsuit as to what they can do there.

Mr. PLATTS. And related to that, the Social Security Act limits your access to the Department of Health and Human Services data base or national repository of wage and employment information?

Mr. MILLER. That's the—I believe what we are referring to there, the new hire date, so-called new hire data base. We actually do use it in some of our work today. We are permitted by law to use it in some fashion and we would be more than willing to walk through that with you as well, and what we might need in terms of additional authority or resources.

Mr. PLATTS. If we're talking about the same thing, Mr. George, correct me if I am wrong, that the use is just related to the earned income tax credit.

Mr. MILLER. Right now it is.

Mr. GEORGE. That's correct. They have the ability to do that, but you touched on a very important point, Mr. Chairman. If they were given expanded access to an HHS data base, this would help address whether or not someone had wages that they could then cite early to try to prevent a legitimate taxpayer later on from claiming their legitimate return. So they do need expanded authority in that area.

Mr. PLATTS. Commissioner, that's a perfect example of how, in reference to Mr. Towns' opening statement, how we want to partner with you, with the IRS, with the IG, with Justice, you know, in identifying; because I want to emphasize, I know there's a very, very good faith effort being made by you, by the Commissioner, to combat this challenge and some of its resources, some of its authority.

But, you know, where you need additional resources or a reallocation of your resources, additional authority, we need to hear that. And so we welcome that feedback of how we can partner with you, and this gets us specifically with statutory authority to allow you to have that information that allows you to better, up front, prevent the fraud from occurring.

Mr. MILLER. And we welcome that discussion.

Mr. PLATTS. I yield to the gentleman from Virginia, Mr. Connolly, for the purpose of questions.

Mr. CONNOLLY. I thank the chairman, and welcome. Mr. Cimino, by the way, from New England?

Mr. CIMINO. No, I'm from—excuse me, Congressman I'm actually from Pittsburgh, sir.

Mr. CONNOLLY. Okay, fully rounded Os. Good for you.

We've looked at, as Mr. Towns indicated, an almost exponential increase in the number of identity thefts related to tax administration: 51,000 in 2008, only 3 years ago; 10 times that number today, 582,000 in 3 years. That can only be described as exponential growth.

And, Mr. Miller, if I understood you correctly, previously you indicated you had to transfer about 400 people to try to deal with that; is that right?

Mr. MILLER. We have, yes.

Mr. CONNOLLY. Pardon me?

Mr. MILLER. We have; yes, sir.

Mr. CONNOLLY. And those are—have you hired new people to handle this problem?

Mr. MILLER. Right now we are going at risk budget-wise for those individuals.

Mr. CONNOLLY. I can't hear you.

Mr. MILLER. I'm sorry. Right now we are going at risk. I'm not sure how we're going to pay for those, but we'll find a way.

Mr. CONNOLLY. Okay.

Let me ask a question maybe to Mr. Cimino, but any of you: Is there sort of a back-of-the-envelope rule of thumb that for every new IRS person or agent we hire, X amount of revenue goes with that person? If we, the Congress, make an investment in the IRS in terms of personnel, what kind of return on that investment can we expect? I mean, if I—you know, it's not the same at HUD. But at IRS there's a certain expectation it enhances revenue.

Mr. MILLER. I think, sir, the question is better answered by me. But I think that—I don't know the exact number but it's a multiple of—it's a positive investment for the Federal——

Mr. CONNOLLY. Absolutely. Would you get back to the record for us?

Mr. MILLER. We will.

[The information referred to follows:]

[NOTE.—The information referred to was not provided.]

Mr. CONNOLLY. And we understand it's not a hard and fast rule but it's a sort of, as I said, back-of-the-envelope calculation that every dollar you put in, you reap $1.75 back, whatever it is.

We had a little discussion before and the chairman is right that the legislation—not his view, mine—ill-advised legislation we adopted yesterday was a novel management principle, that by freezing and capping personnel in any enterprise, somehow that's a good thing.

I have yet to find a single corporation in America that would agree with that, that just arbitrarily saying we are going to cut back 10 percent and stay there.

And if you want to replace anybody, irrespective of criticality of mission, you know, it's going to be on a one-to-three ratio. And the disruption to missions, you know, so be it. Now it is true, as the chairman indicated, that that's a global number, but it's also naive to believe that wouldn't affect IRS. IRS is hardly the favorite agency of the majority in this Congress.

So I doubt very much that you're going to get a carveout. Yesterday when there were amendments, we refused to have a carveout for veterans. We refused to have a carveout for, you know, criminal prosecutions and public safety activities. So why we would have a carveout for IRS, I don't know.

But let's just posit theoretically that the impact of that legislation were to become law on IRS. So let's say, by attrition, over the next 3 years by the way, you lose 10 percent of your current work

force, what would be the impact on identity theft if you had to—not only you are looking at, Mr. Miller, trying to find 400 people to serve this exponential growth problem, but now on top of that, how about a 10 percent reduction?

And it could be worse. What the chairman says is absolutely correct but the obverse is also true. You might have to take a bigger cut because some other agencies are considered priorities, and they don't—there are not sustaining the 10 percent cut.

Mr. MILLER. I guess it's a difficult—it's a difficult question to answer.

Mr. CONNOLLY. No, you have to answer it. We passed this bill yesterday, so you have to start thinking about how would I implement such a bill which could have, under worst-case scenario, a 10 percent reduction in the work force.

Mr. PLATTS. Would the gentleman yield?

Mr. CONNOLLY. Yes.

Mr. PLATTS. I would like to add one clarifying aspect about the bill is that it does provide the CEO, the President, the waiver authority for the efficient operation of any agency or for critical missions of an agency to exceed that cap, so it does allow—so if the President thought the IRS needed additional, I just wanted to note that that was part of the language of the bill.

Mr. CONNOLLY. And I thank the chairman for that clarification, and he is correct.

However, I would point out that that is an extraordinary waiver. In other words, we don't go to the IRS administrator to make a judgment; we go all the way to the President of the United States in the White House.

Good luck, Mr. Miller, in getting a waiver from the White House for your operation. You know, "We need 10 extra people, Mr. President. Will you sign a waiver so we'll get around this provision in this law?"

I think that's an extraordinarily high level and I think, frankly, it doesn't really solve micro-problems like the one we're dealing with here, even though they're growing exponentially.

Mr. Chairman, I know my time has expired, but I wonder if you would just allow the witness to answer the question and then I will be done. Thank you.

Mr. MILLER. So I—obviously a 10 percent cut would be a material reduction in our force and that's happening already, by the way. Over——

Mr. CONNOLLY. Mr. Miller, time is limited. Of course, that's true. That's self-evidently true.

My question is: What does this do to your mission given the fact that we've had a 10fold increase in 3 years in identity theft with respect to tax administration that you are trying to deal with? If we have a 10 percent reduction in the work force, how would that affect your ability to deal with this exponentially growing problem?

Mr. MILLER. We will have to decide where we take those cuts, Congressman, and I don't know whether they will be—but we will have to take cuts, yes.

Mr. CONNOLLY. And presumably that would impair your ability to respond to this growing theft.

Mr. MILLER. It will force some very tough choices, no question about that.

Mr. CONNOLLY. Thank you very much. Thank you, Mr. Chairman.

Mr. PLATTS. The gentleman yields back. And we do have a difference of opinion what the bill means. As one that believes we—Congress and the President—need to better prioritize where we put our resources, and enforcing our tax laws is one of those priorities. But I respect the gentleman's opinion.

But I think the gentleman started to say that you've had a reduction.

Mr. MILLER. Right.

Mr. PLATTS. And I would hazard a guess that that's related to advances in technology in the last, say, 10 years; that because of technology and computers, a lot of what we do today, and when we are talking about filters, is not manual review but electronic review of data.

Mr. MILLER. Well, yes and no, Mr. Chairman, because taxpayer rights are such that I can't just look at a return on the computer and say it's a bad return. There's always a treatment stream after that that involves a person.

Mr. PLATTS. Absolutely. But that initial review maybe is done electronically as opposed to manpower.

Mr. MILLER. Most of it is electronic at this point, some of it is manpower. But certainly the back end of it is, once you find you have to do something with it, as we talked about with the victims and everyone else, it needs to be worked to ground by people.

Mr. PLATTS. Absolutely. I appreciate that, especially when you get into that type of detail.

I yield to the ranking member, Mr. Towns.

Mr. TOWNS. Mr. Chairman, we have a vote on, so I am going to not ask my questions be answered at this point but to ask them to respond to us in writing, if that's okay with you.

IRS can't give information, even to States or local law enforcement, that may be investigating or prosecuting identity theft crime under a State criminal statute. Each of the offices represented today has to deal with this law. So if I could get you to respond to these questions in writing for me, I would appreciate it.

My question is: Why is this law that was enacted to deal with crime 40 years ago, still preventing the prosecution of new escalating criminal schemes?

Number two, what would be an appropriate legislative response to certain sections of 6103 provisions that can enable you to do your job of stopping these crimes more effectively?

Number three, have there been proposals from any of your offices on adjusting section 6103 to meet the needs of your agencies in combating identity theft crimes?

And the last one: What consequences, both negative and positive, would such a legislative remedy have?

I would appreciate that. And being my voting record is not the strongest, I need to go make this vote, Mr. Chairman.

Mr. PLATTS. The gentleman yields back.

I am going to try to wrap up with three main areas here and then we will conclude the hearing, and appreciate the additional information that will be provided in in writing.

The first is on the issue of the reference of $4.2 billion in fraudulent child tax credits. And it's my understanding that the IG is identifying those as paid to individuals here illegally; is that correct, Mr. George?

Mr. GEORGE. Well, I would say paid to people who use I–10's, not Social Security numbers, and our research has indicated that most people who use the I–10 are not in the country legally.

Mr. PLATTS. Okay. So a high propensity of these are likely here illegally.

Mr. GEORGE. That's a reasonable conclusion.

Mr. PLATTS. And my understanding from your written testimony is that of that $4.2 billion number that you have identified, that to your belief, that none of that has been recovered?

Mr. GEORGE. Yes, that's correct, sir.

Mr. PLATTS. Commissioner Miller, anything you can share on efforts—and we're talking about not even millions now, but billions of dollars of fraudulent payments, taxpayerfunds, have gone out to likely illegals; and obviously, you know, there's individuals who intentionally, you know, are violating the law to seek that money. But is there an ongoing effort to recover it and, if so, what success are we having?

Mr. MILLER. So I think I would—we will get back to you more fully in writing.

I don't think we agree with the number, to start with. We don't agree that it's all fraud, and we do have an enforcement effort underway. I don't want to say that either. We are working on—because some of it is fraud, there's no question. Some of it is mismatching.

And by the way, when you talk about I–10 holders, that would be a change of law that you all in Congress would have to make because that's not a barrier to getting the credit. So it's a more complex sort of answer that I'm more than willing to come back in in much more detail on.

Mr. PLATTS. And if you can give us—why do you disagree with the number, you know? I'm glad if you want to do it in writing.

Mr. MILLER. Yes, we'll do that in writing.

[The information referred to follows:]

[NOTE.—The information referred to was not provided.]

Mr. PLATTS. But what do you find inaccurate in what the IG's finding is? And then, specifically, you referenced something that we would have to do to prohibit somebody here illegally, if there's something we're missing in the law, because it's certainly not the intent of Congress and my belief and certainly not what I think should be our intent—should not be our intent that—if you're here illegally, that you get the benefit of a tax credit from the general Treasury. So if there's something that we should look at as far as, again, a statutory change, I would welcome that suggestion, that recommendation.

Mr. MILLER. Absolutely.

Mr. PLATTS. The issue of the number of tax refunds that are deposited in the same bank account, again in the IG's testimony ref-

erenced in 2008, the IG reported that IRS had not yet developed a process to ensure that more than 61 million tax refunds were deposited to an account in the name of the actual filer, as required by Federal direct deposit regulations. And an analysis of the direct deposit data for 2007 showed that more than 700,000 bank accounts received three or more tax refunds totaling $8 billion.

I can think of times where more than one account, a family, and perhaps a teenager working, or somebody doesn't have a bank account—although today I would encourage they should; as I referenced to you yesterday, both of my sons, 15 and 12, have their own bank accounts—but where there could be instances.

But are we, you know, being dutiful here in identifying if one bank account is getting 10 or 20 or 30 accounts a day that's, again, to me, a huge red flag that should go up that there's something askew here.

What, if anything, are we doing to better address this issue that the IG raises in their testimony?

Mr. MILLER. So, a couple of things. And again this might be something, again, that we're going to go to you back in writing on, because it's not something I really want to discuss too widely, but we're doing a few things.

I agree with you that bells and whistles ought to be going off when many, many refunds are going into an individual bank account.

That said, there's no legal barrier to that, I don't believe, but we ought to be doing a better job tracking it and we are going to do that going forward.

We are also working, frankly, with software developers and other financial institutions to try to better the flow of information between all of those parties and the IRS, and that will help as well.

But in terms of what specifically we're going to do, that's something I will be glad to come back to you on.

[The information referred to follows:]

[NOTE.—The information referred to was not provided.]

Mr. PLATTS. Yes. This, you know, is about interactions between the IG and the IRS 3 years ago, you know, 2008, referencing what had happened in 2007. So I realize you were not in your position in 2007 or 2008, but you are today and I appreciate your taking a serious look at it.

And this is one of those, what I'll call triggers, you know, of how to use technology to better identify, you know, intended fraud or attempted fraud. And, you know, that if one bank account, the same bank account is going to get three or four, I mean, the higher the number, the more scrutiny it should get. And I would think that certainly if it's five or more, that should get some great scrutiny. Maybe it's three, but your data probably is going be able to better identify what that threshold should be.

And if we're not doing that, I guess my question is why aren't we? Because you know, again, the best way to protect the victim is to prevent the fraud in the first place. And so what I really—you know, my focus, as I said in the beginning, is when there is a fraud committed, you know, are we doing everything in our power to assist the victim of that fraud to get back, you know,

made whole as quickly as possible? And then up front, how are we preventing the fraud?

And these triggers, I'll call these trip wires that should be sending off kind of warning notices that the more of them that are tripped, the more scrutiny these returns should be getting, and this is yet one more example of the bank account.

Mr. MILLER. One barrier, Mr. Chairman, obviously, is there are going to be accounts that are going to be returned, that are going to receive an awful lot of refunds, absolutely appropriately, some return preparers, some financial providers of refinance anticipation loans and other sorts of things. That will be improved going forward as we roll out our system of actually registering return preparers. We will have a better way to track that than we have in the past.

Mr. PLATTS. The, again, up-front efforts to prevent the fraud, one of the proposals in Senator Nelson's bill that he has introduced regarding this issue is that individual taxpayers have the ability, the option of opting out of e-filing so that somebody can't do it electronically, they have to actually provide written W–2s. Is that something that the IRS is looking at in any fashion or would be willing to consider?

Mr. MILLER. So I think we are just looking at the bill, and I don't have a firm reaction from the administration or even from the IRS. I would say, you know, there would be costs to going back to paper, obviously, and IT costs to having a toggle switch for an individual taxpayer. So those are our immediate concerns, but we will work that.

Mr. PLATTS. Okay. Related to that is instead of going back to paper, staying electronic, but that a taxpayer could request a PIN as opposed to being offered one by the IRS, so that you don't go back to paper, you stay electronic, don't have the increased manpower, but someone who hasn't yet been a victim of identity theft, but while it was stolen and where they may become a victim, and they are trying to be proactive rather than after they've been victimized, "All right, now we will get a PIN."

Where does that type of consideration stand with the IRS?

Mr. MILLER. So one of the changes in 2012 will be not only are we sending out these identity theft PINs to folks that we've validated, but if you come in, "I lost my wallet, and I'm worried," we will take a look to see what your filing requirement is. We will take a look to ensure you are who you are, and you may very well be able to get a PIN. That's something that's rolling out again in 2012.

Mr. PLATTS. So that is going to be an option, or you are looking at making it an option?

Mr. MILLER. I think it's going to be an option. I will have to come back to you, whether it's everyone or whether it's a certain subsection of those folks, but we're moving in that direction.

Mr. PLATTS. Yes. If you can, again, give us a definitive answer for the record; is it an option and, if so, and if not, when will a decision be made as to when it becomes———

Mr. MILLER. I believe it is. But let me verify.

[The information referred to follows:]

[NOTE.—The information referred to was not provided.]

Mr. PLATTS. Thank you. A final question. My understanding—well, back in January you began looking at how to better address the issue of identity theft and the fraud related to it, and that you plan on issuing two reports, one on the assessment of the current state of your identity theft program and one on the future state, where you're going to go.

Are those reports near completion?

Mr. MILLER. So I had seen that in a prior testimony, and I will have to take a look and figure out what's going on with those. There are obvious—we have a couple of teams. One has worked and focused on the front-end prevention. One has worked on making the victims less victim-like as they go through our system. Whether they have actual reports—while I have seen many decks, whether there's actual reports we will have to come back beyond.

Mr. PLATTS. If you could give us the status of those reports, because it sounds like internally you're seeking to do, based on my understanding, what we're after; which is, to get a better handle on your efforts, you know, in the big picture, of what you're doing proactively, how you're responding to fraud, how you're handling and assisting victims. So we welcome that information.

Mr. MILLER. Absolutely.

[The information referred to follows:]

[NOTE.—The information referred to was not provided.]

Mr. PLATTS. I will give each of you, if you have any final comments you want to make sure are part of the record, there's something that I did not address or the other members of the panel did not address.

Mr. GEORGE. Mr. Chairman, I would just simply note that TIGTA is in the process of taking a review of the IRS' action as it relates to identity theft forward, and we anticipate two reports in the early spring and late summer, or late spring and early summer.

Mr. PLATTS. We would look forward to receiving those as well. I think the more information we all have of the current situation and where we're heading and how to do better by the American people, the better off the country is going to be financially, and taxpayers are going to be from being prevented from being victimized.

Mr. Cimino.

Mr. CIMINO. Mr. Chairman, on behalf of the Department, we're pleased to be here and try to deal with some of these really critical issues that the subcommittee has focused on, and I will respond on behalf of the Department to the questions of the ranking.

Mr. PLATTS. Thank you, Commissioner Miller.

Mr. MILLER. I am happy to be here and will look forward to working with you and the staff.

Mr. PLATTS. Generous of you to say "happy to be here" when you are being put on the hot seat. And I know that it's probably less fun to be in those seats versus up here asking the questions. My hope is that each of you understand that it's not to put you on the spot, but really to just generate a dialog and, you know, that we really, you know, get everything on the radar that we think needs to be addressed.

As an oversight committee, our role is to raise questions and to get answers to those questions of how we can make government in

total—in this case the IRS—more efficient, better serving the American people.

I certainly understand that all three of you and your colleagues seek to do that every day and in no way want to suggest that you're not.

Sometimes it helps when you have an outside set of eyes or input, you know, kind of get you to look at things outside of maybe that typical box, and that's part of the intent of this of hearing.

As I said earlier, our hope is that we will be better successful—more successful on preventing fraud, protecting tax dollars, but when it does occur, better assist the victims. And in our June hearing it came through that we had not done a very good job of aiding those who had been victimized. And, you know, we clearly need to do much better while protecting the tax dollars of all Americans.

So we'll keep the record open for 14 days for the additional information that you're going to provide. And if we have any final questions that we didn't get to, also we'll get them to you in a timely fashion. But we're grateful for your testimony here today and, again, your workday and a day out, as well your colleagues and your various departments and your agencies, and we know we're on the same team trying to do a good job for the American people.

This hearing stands adjourned.

[Whereupon, at 11:32 a.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

**"Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service"**
Hearing on November 4, 2011

**Questions from Rep. Todd Russell Platts, Chairman**
**Subcommittee on Government Organization, Efficiency and Financial Management**

Question 1

Victims who have their identities stolen may spend months or even years trying to resolve the problem. Identity victims have expressed their frustration at excessive delays, having to submit duplicative paperwork, and being referred to multiple components within IRS before getting assistance.

Q: What is the average resolution time for a case of identity theft?

In FY 2011, all identity theft work resolved in Accounts Management, including those cases resolved within the Identity Protection Specialized Unit, averaged 178 days. Those identity theft cases involving duplicate return filings, where two or more returns are filed using the same social security number, averaged 196 days in FY 2011. This time frame includes the potentially substantial time lapses between when the IRS sends written correspondence in the mail, and when the taxpayer responds via mail with the requested documentation. We recently added 200 people to work identity theft cases, bringing the total to 400 people, to reduce the average time to resolve identity theft cases and expect resolution times to improve going forward.

Q: What is IRS doing to better assist taxpayers who have their identities stolen, and why hasn't the IRS prioritized its assistance to identity theft victims?

The IRS has prioritized this area. The IRS has made great strides in improving the identity theft program. The IRS will continue to prioritize identity theft in the future and increase customer service to the taxpayer, while making it more difficult for identity thieves to commit fraudulent acts.

The IRS established a dedicated team to conduct a service-wide review of all identity theft processes and procedures related to the treatment of identity theft victims. That review led to the implementation of a number of process improvements that allow more timely resolution of taxpayer cases and better identification of identity theft on incoming tax returns. The IRS is working with both internal and external stakeholders to proactively identify new schemes and

situations where taxpayers are impacted by identity theft. The IRS is continually developing new identity theft indicators and associated treatment streams to both protect and reduce or eliminate the burden and inconvenience associated with identity theft often experienced by the taxpayer.

Examples of process improvements and ongoing initiatives include:

- Implementation of specialized identity theft units within each business unit (e.g. the business units that deal with individual income taxes, business taxes, etc.), which will allow IRS to address the impact of the identity theft issue, adjust accounts to make the taxpayer whole where necessary, and work with the taxpayer to protect them from future problems. A specialized unit in each business function will greatly reduce the need to transfer cases to other functions to be worked, thus reducing the time necessary to complete the case. This will also allow employees with specialized skills in both identity theft and business unit issues to work the case to completion with a single point of contact for the taxpayer.
- Implementation of mandatory identity theft training for all IRS public contact employees who work with taxpayers that may be affected by identity theft.
- Implementation of increased internal controls to allow IRS to better track identity theft cases so that inventories are worked in a timely manner.
- Expansion of the Identity Protection PIN (IP PIN) to more than 250,000 taxpayers who have previously been identified as being the victim of identity theft. This IP PIN will allow IRS to more effectively identify fraudulent returns while, at the same time validating that the return filed is the taxpayer's legitimate return.
- Implementation of new codes to systemically identify fraudulent tax returns using deceased taxpayer information.
- Implementation of a new special processing code for returns with identity theft documentation attached that will allow for systemic identification of potential victims.
- Review and revise, as appropriate, all Internal Revenue Manual sections to promote consistent treatment of all identity theft cases throughout the IRS.
- Increasing taxpayers' awareness with targeted information about identity theft; tips and suggestions for safeguarding their personal information, and information to help them better understand tax administration issues related to identity theft. The IRS issues tax tips, such as *"Ten Things the IRS Wants You to Know about Identity Theft"* on IRS.gov as part of our external communications during the filing season.
- Collaborating with external stakeholders, such as the Federal Trade Commission, the Federal Identity Theft Enforcement Interagency Working Group, and the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center, to provide guidance on identity theft prevention and resolve the challenges posed by the growing threat of identity theft.

The IRS is also increasing the number of resources dedicated to working identity theft cases. With the increases, 400 employees are now focused on the resolution of identity theft cases. The employees added in FY 2011 alone resulted in 134 percent more case closures than in FY 2010.

Question 2:

In 2011, IRS ran a pilot program testing the efficacy of personal identified numbers (PINs). The PINs were made available to taxpayers who had been victims of identity theft in previous years as a way to provide an extra layer of security to their tax returns.

Q: What was the result of the 2011 PIN pilot program?

IRS implemented a pilot program for the 2011 Filing Season to test IRS processes and procedures for tax returns that contain an identity theft indicator. If the taxpayer filed his or her electronic or paper return, and provided the unique IP PIN on the appropriate section of their return, it allowed easier processing of the return.

The pilot taxpayer population was limited to those taxpayers where the IRS was confident that we had properly identified the legitimate taxpayer and had the correct address of record for the legitimate taxpayer. Each taxpayer was sent a notice that contained a unique IP PIN tied to that specific taxpayer's account and instructions as to how the IP PIN was to be placed on the tax return. This notice was scheduled to be sent in January 2011; however, due to unexpected systems issues, notices were not sent to taxpayers until the first week of February. As of the date that the notices were sent, more than half of those taxpayers had already filed returns. Approximately 17 percent of the remaining taxpayers used the IP PIN correctly. Because 2011 was the first year of the program and notices were sent after the start of the filing season, we believe that the results are not representative for future years and usage will improve going forward.

Based on the 2011 pilot results, IRS took several actions to enhance the programs for the 2012 filing season. These include the following:

- IP PIN notices will be delivered prior to the filing season.
- The Notice language was improved and written in a more detailed, clear and concise manner.
- The Form 1040 was modified to specifically accommodate the IP PIN.
- Increased communication to taxpayers, software developers, and tax preparers prior to the IP PINs being sent to ensure all stakeholders were aware of the program.

Q: Will IRS increase access to IP PINS in 2012 and if so who will be eligible to receive PINs?

Yes, IRS expanded the IP PIN pilot and enhanced the functionality which enabled us to increase access to over 250,000 taxpayers.

Question 3

The amount of tax returns filed online has increased exponentially over the last five years. In many cases, fraudsters are using electronic returns and commercial software as a way to file numerous fraudulent returns quickly.

Q: Do electronic returns allow people to file fraudulent returns more quickly than paper returns?

Electronic filing provides benefits for both taxpayers and tax administration. For taxpayers, electronic filing provides convenience and faster refunds. For tax administration, electronically filed returns cost less to process than paper returns and they allow for the transcription of more data from returns, which benefits both enforcement efforts and the ability to provide service to taxpayers. The Government Accountability Office highlighted these benefits in its recent audit report titled "E-Filing Tax Returns – Penalty Authority and Digitizing More Paper Return Data Could Increase Benefits" (GAO-12-33). While it is true that refunds from electronically filed fraudulent returns can be paid faster than refunds from fraudulent paper returns, fraud occurs both on paper and electronically. All returns, whether filed on paper or electronically, are subject to the same compliance filters.

Q: Is the rise in tax fraud at all related to the rise in electronic filing? If not, what contributing factors have impacted the rise in tax fraud since 2008?

Overall fraud, including identity theft, has become more prevalent over the last few years as identifying information is more easily obtained through outside sources by outright theft, online phishing, scams, and stolen social security numbers used by people other than the legitimate taxpayer. As identity theft increases, the incidence of identity theft fraud goes up. The increase in tax related fraud is one example of the misuse of identity information. There is, however, no data to support that electronic filing is a creator of tax fraud, as tax related fraud occurs in both paper and electronically filed returns.

Q: What information is needed in order to file a return online?

Anyone can file their tax return online through the different e-file options (Free-file, Fillable Forms, with commercial tax software, or through a paid tax preparer). There are exceptions in cases where a taxpayer is claiming a tax benefit that requires paper documentation to be attached to a return or when a taxpayer is required to attach a form to their return that is not e-filable. Other exceptions are if the taxpayer is filing an amended return, a fiscal year or prior

year return, or if the taxpayer is filing under a temporary identification number issued by the IRS.

In order to e-file, the taxpayer must provide the names and taxpayer identification numbers (for themselves, or both spouses if filing jointly, and any dependents) and an address. Checks are performed to ensure the name and Taxpayer Identification Number (TIN) match information in our system before the return will be accepted.

Taxpayers are also required to enter either the prior year's Self-Select PIN or the prior year adjusted gross income (AGI) to verify their identity. Taxpayers who don't have prior year information can obtain a temporary Electronic Filing PIN. To obtain an Electronic Filing PIN, taxpayers use either the online tool or call the IRS and provide the following information: Social Security Number or Individual Taxpayer Identification Number; first and last name; date of birth; filing status; and complete mailing address as it appeared on the prior year's tax return.

In addition, taxpayers should be aware of other pieces of information included on a return – for example, the taxpayer should have his or her income information, dependent information, deduction and credit information and payment information (either to pay a balance owed or bank information if a direct deposit is requested), but each piece of information is taxpayer specific.

Q: As more people are filing their taxes electronically, what is IRS doing to ensure that their information is secure and that fraud is identified?

IRS has a robust policy for protecting taxpayers' personally identifiable information. Systems are in place to ensure that taxpayer data sent to the IRS is secured. All electronic filers are subjected to the electronic filer application process to protect taxpayer data.

IRS has multiple compliance filters in place to identify fraudulent or erroneous returns received during processing of both electronic and paper returns. We also perform reviews of return information during pre-refund stages and post-processing of tax returns, and income information that apply to both paper and electronic returns. Areas such as the Accounts Management Taxpayer Assurance Program, Compliance Examination, and Criminal Investigation have established procedures to identify or work fraud related issues. The IRS Identity Protection Specialized Unit (IPSU) has been established to provide unique support to taxpayers to assist with navigating the IRS processes on issues related to identity theft.

Question 4

IRS has mentioned several new initiatives it has taken to better identify and prevent fraud. These initiatives include registering tax return preparers and increasing the accuracy of filters to identify fraudulent returns.

Q: What are IRS's current filters for identifying tax fraud, especially identify theft?

The IRS uses the Electronic Fraud Detection system to identify possibly fraudulent returns. This system relies on data mining scores, fraud models and algorithms to determine the likelihood of fraud. The IRS uses a process of income verification as part of assessing the risk of whether a return is fraudulent. The models and algorithms consist of numerous characteristics of fraud, and are constantly updated. Currently the models focus on all types of fraud, however, IRS has built a new identity theft model for next filing season. The new model is based on information learned from previously identified identity theft returns with the goal to identify identity theft returns before they are processed.

Q: What is the status of IRS's process to register tax return preparers?

As of November 15, 2011 approximately 750,000 preparers have registered with the IRS. This group includes CPAs, attorneys and enrolled agents as well as about 460,000 previously unenrolled preparers. Many of these unenrolled preparers will be required to take a competency exam which is now available. Once individuals have passed the test and a tax compliance check, they will become Registered Tax Return Preparers. In addition, continuing education requirements for preparers are slated to start early in 2012. The IRS is working closely with many tax professional organizations during the implementation process to ensure their input is considered as the program moves forward.

Q: What is IRS doing to address the problem of tax returns issued to deceased individuals?

The IRS has existing filters in place to identify decedent returns filed for taxpayers who died prior to the current tax year. Because tax filings are appropriate for the year of death (taxpayers' estates are frequently required to file a return the year after death), filing a tax return on behalf of an individual who is deceased does not necessarily indicate fraud. However, recognizing the increasing use of decedents' SSNs for the commission of tax fraud, the IRS put specific filters into place to identify fraudulent returns involving decedent returns. We stopped the refunds, verified the identity of the taxpayer, and if not verified, we marked the account for identity theft. For next filing season, the IRS will also put into place new programming that will cause the returns of recently deceased individuals to be identified during processing for manual review before any refunds are issued.

Question 5

In past years, IRS has used third-party sources to verify the accuracy of its payments, such as with the First Time Homebuyer Credit. Using existing data from both the government and the private sector could reduce improper payments and fraud.

Q: Since 2008, how often has IRS used data from the private sector to verify the accuracy of IRS payments? For what programs was the data used, and what were the results?

The IRS uses third party data for a variety of purposes, including helping verify refundable credits. We do proceed cautiously in some cases, however, as there have been issues with reliability of certain third-party data.

First-Time Homebuyer Credit: The IRS recently utilized third-party data in work on the First Time Homebuyer Credit (FTHBC). In April 2010, the IRS received data from a third party property provider for 1.7 million taxpayers who claimed the FTHBC. The provider aggregates data from public record data sources, such as county tax assessor's offices. While this third-party data is helpful, it required a significant amount of validation, analysis, and filtering by the IRS to be useful. After this was completed, the data results were compared to internal data to validate home purchases for taxpayers that claimed the First Time Homebuyer Credit. IRS identified discrepancies with reported purchases and the third-party data and referred returns for audit.

Additional stratification of combined internal taxpayer data with third-party data identified taxpayers that may be required to report dispositions and repay the credit. Taxpayers received reminder notices on how to report dispositions and their obligation to file and report a change to their main home.

Questionable Refund Program Employer Information: The IRS has secured advance wage information from some large employers, which is used to screen questionable claims during processing as part of our Questionable Refund Program. We intend to increase our use of this third-party data into the filters.

Q: Does IRS use information from government databases such as Social Security Administration Death Master File or the Department of Treasury Debt Check Database? What databases does IRS use and what impact has the data had on identifying fraud and improper payments?

The IRS uses the Treasury Debt Check Database. Any refunds due to the taxpayer will be offset to pay the debt first. Any fraudulent refunds that are offset will be returned to the IRS.

Additionally, IRS uses the following information from government databases:

Prisoner Information

The IRS maintains a database containing information about prisoners using information provided by the state departments of correction and the Federal Bureau of Prisons. The IRS uses this information to stop fraudulent prisoner claims. Previously, the information was provided voluntarily. Now, as a result of the United States-Korea Free Trade Agreement Implementation Act, the Federal Bureau of Prisons and state departments of corrections are required to provide certain prisoner information to the IRS in an electronic format. The IRS expects this information to be more helpful in identifying fraudulent prisoner refunds on a going-forward basis.

In FY 2011 we stopped over $2 billion in false or fraudulent prisoner refunds using the prisoner file to assist us in detecting questionable returns.

Numident

This data file, provided by Social Security Administration (SSA), contains information relating to individual social security numbers (SSNs). We use this information to validate and match names and social security numbers for a variety of purposes. SSA provides IRS weekly information on additions, deletions and updates to the file.

The IRS uses the Numident data to systemically screen income tax returns claiming child-related tax benefits. For the Earned Income Tax Credit (EITC), the IRS uses the information to screen for valid SSNs and EITC eligibility requirements including age and relationship.

In addition, we receive a copy of the death master file on a weekly basis from SSA. The date of death information is used to stop decedent returns in processing for taxpayers who died prior to the tax year. See Question 4 for more comprehensive information on efforts related to deceased taxpayers.

Federal Case Registry (FCR)

This data file, maintained by the Office of Child Support Enforcement (OCSE), Administration for Children and Families, U.S. Department for Health and Human Services (HHS), contains information on state child support orders. The information includes data regarding custodial party and non-custodial parent and children involved in cases where a child support order has been established or modified after October 1, 1998 and cases where the state is providing child support services.

The IRS uses the FCR data to systemically screen income tax returns claiming child-related tax benefits. While there have been reliability issues which prevent IRS from using this data as the sole reason for a math error adjustment (as the law allows), when used with other filters, it has been successful in selecting returns for audit.

National Directory of New Hires Database (NDNH)

The IRS systemically requests wage information from the NDNH database, verifies employment and then manually validates earned income for selected EITC returns. This database, owned by HHS, contains quarterly wage information on all wage earners, not just new hires.

Currently, the IRS has legislative authority via Title 42 USC 653(i)(3) to use the NDNH database for the purpose of administering the EITC. IRS uses that authority to match income on returns that are flagged by the Questionable Refund Program as potentially fraudulent refund claims. The authority does not currently extend to use of the data to administer non-EITC returns.

Additionally, we would note that Treasury is conducting a pilot project to assess whether data maintained by states could assist in identifying both ineligible individuals who receive improper EITC payments and eligible individuals who are not claiming the EITC. This effort is being worked as part of the Office of Management and Budget Partnership Fund for Program Integrity.

Q: How successful has third party data been in reducing improper and fraudulent payments?

As discussed above, third party data can be very valuable when it is information that directly ties to credit eligibility requirements, is reliable and available as early as possible in return processing.

Question 6

The Treasury Inspector General for Tax Administration (TIGTA) issued two reports in 2011 finding that IRS had improperly issued tax credits, including $4.2 billion in Earned Income Tax Credits.

Q: What is IRS doing to prevent the improper issuance of tax credits?

The IRS has a multi-faceted strategy to address tax non-compliance in the form of improper claims of tax incentives.

In implementing compliance actions related to refundable credits the IRS assesses the risk associated with the credit and develops strategies that address those risks. With the expansion of refundable credits in recent years, we have used lessons learned to improve our administration of the credits.

The IRS looks to identify problems as early in our process as possible. All refundable credits go through various filters where we match them with certain pieces of information during return processing to identify potentially erroneous credits.

When the law allows, we apply math error authority which allows us to immediately make adjustments to the returns without conducting an examination. We have general math error authority for errors in computation, use of incorrect SSNs, claims for more than the statutory limit, etc. We also have specific math error authority, granted by law, to deny the FTHBC to taxpayers who do not meet the age requirement, who have provided information on a tax return for at least one of the two preceding taxable years which is inconsistent with eligibility for the FTHBC, or who fails to attach required documentation to their return.

Returns are processed through our Electronic Fraud Detection System (EFDS) which is designed to identify potentially fraudulent schemes and suspicious patterns. For returns identified as questionable by the EFDS, the refunds are frozen and are reviewed by a team of employees before refunds are released.

IRS also conducts examinations of questionable returns, selecting them based on business rules and using available third party data, like the Federal Case Registry. Many of our examinations are conducted while we hold the refund. For FY 2011 we conducted a substantial number of examinations on the largest refundable credits including almost 484,000 EITC examinations protecting over $2 billion in improper refunds claimed. In FY 2011 we closed almost 200,000 FTHBC examinations protecting almost $517 million, and over the life of the credit closed over 500,000 examinations protecting almost $1.7 billion. For the adoption credit, we closed almost 45,000 exams protecting almost $256 million.

We also match the information returns filed by employers reporting wages and non-employee compensation when they become available to the income reported on income tax returns. In FY 2011 we closed over 1 million EITC cases identified through matching, protecting over $1.3 billion.

The IRS is taking a number of other actions to reduce erroneous EITC payments. These include the following.

1. New Return Preparer Initiative – Under this groundbreaking new program, paid tax return preparers are now required to register with the IRS and complete certain continuing education and testing requirements. Under the former regime, the IRS did not have oversight over all tax return preparers as anyone could

prepare a tax return for compensation. This initiative brings all tax return preparers under the ethical rules imposed on those who practice before the IRS and subjects all preparers to oversight by the IRS. We have the ability to remove or suspend problematic preparers from preparing returns. Note that almost two thirds of EITC returns are prepared by paid preparers. Testing and enforcement strategies will include a focus on EITC issues. While difficult to measure precisely, the IRS expects these return preparer initiatives to improve overall EITC accuracy. We expect to have a better sense of the magnitude of the new Return Preparer Program after the conclusion of our three year ramp-up and after we develop baseline measures.

2. Due Diligence Checklist – Beginning with the next filing season (2012 filing season; 2011 tax year returns), EITC returns prepared by paid tax returns preparers will be required to include the existing due diligence checklist with the filed return. This will help ensure that preparers are taking appropriate due diligence steps in the preparation of returns. Under current rules, tax return preparers are only required to retain a copy of the checklist for their records.

3. Increase in EITC Due Diligence Penalty – The Administration's FY 2012 Revenue Proposals included a proposal to increase the present law penalty on tax return preparers who fail to comply with the EITC due diligence requirements from $100 to $500. The increased penalty was enacted effective for tax year 2011 returns.

4. EITC Specific Preparer Strategy – The IRS continues to refine and evaluate our focus on activities associated with a variety of actions to encourage compliance by EITC paid preparers, based on risk-based selections, including due diligence audits, visits by revenue and criminal investigation agents, injunctions, and educational and compliance notices to first-time and experienced preparers to influence the accuracy of EITC returns filed.

   The IRS also balances our compliance approach with a significant number of outreach and education activities for refundable credits. We have robust communication strategies that leverage communication channels and marketing. We partner with hundreds of community-based organizations across the country to provide education and outreach about credits, supporting free tax preparation at volunteer income tax assistance (VITA) and AARP operated Tax Counseling for the Elderly (TCE) sites around the country. IRS also provides outreach and education to the paid preparer community. We also work with tax professionals and tax professional associations to ensure tax preparers have the tools they need to prepare accurate returns.

Q: Does IRS agree with TIGTA's assessment that $4.2 billion in EITC and $3.2 billion in education credits were issued improperly in 2011. Please explain.

The $4.2 billion referenced by TIGTA in 2011 related to the Additional Child Tax Credit (ACTC), not the EITC. The IRS disagreed with TIGTA's finding that $4.2 billion in ACTC were issued improperly. It is important to recognize that unlike many other tax benefits, the law does not require the taxpayer or eligible child to have a social security number (SSN) in order to receive the Child Tax Credit (CTC) or ACTC. We are administering these credits according to the law. TIGTA's findings include claims that were, consistent with the law, paid to those who filed with Individual Taxpayer Identification Numbers (ITINs), not SSNs.

Regarding the TIGTA report on the American Opportunity Tax Credit (AOTC), the IRS disputes the TIGTA analysis, as the numbers of erroneous claims for the AOTC are overstated. The report based the bulk of its findings on an inability to match tax returns with the corresponding Forms 1098-T, Tuition Statement, information returns filed by colleges and universities with the IRS. The absence of this form or an incorrectly completed form does not in and of itself mean the taxpayer is ineligible for the credit. However, despite our objections to the findings of the report, no amount of fraud is acceptable, and the IRS has already begun to take steps to increase monitoring and improve compliance, including the following:

- Working with educational institutions and other outside stakeholders to improve the accuracy of their reporting.
- Increasing the number of unmatched returns that will be reviewed in future years. Resources have already been allocated to recover potentially erroneous credits for students with no documentation.
- Examining those returns where we see the greatest potential for erroneous claims.
- Revising the reporting requirements and tax forms so that the IRS receives additional information that will assist the IRS in determining who legitimately qualifies for education credits. Form 8863, on which the AOTC is claimed, will be revised for tax year 2012. Beginning in 2012, taxpayers claiming an AOTC will be required to identify the school they attended. Also, taxpayers will receive more information to verify their own eligibility prior to filing.
- Revising Form 8863 for TY 2012 to capture 1) the education institution identifying information (allowing matching) and 2) eligibility information that will guide taxpayers through the eligibility determination (i.e. clarifying half-time and four year post-secondary status).
- Working with the Department of Education to determine the feasibility of obtaining information from their databases and to assess if this data could be used during tax return processing to assist in verifying eligibility for education credits.

**Questions from Rep. Edolphus Towns, Ranking Minority Member Subcommittee on Government Organization, Efficiency and Financial Management**

Question 1

Many of the initiatives the IRS has implemented to deal with tax-fraud and identity theft, involves Information Systems. Centralizing the ID theft complaint and resolution centers requires an IT system that is capable of handling the data. Tracking and reporting incidents of ID theft fraud also requires a fluid IT system.

Q: When last did the IRS upgrade its information systems?

The IRS routinely makes custom software enhancements throughout the course of the year to its fraud detection systems. In June 2011, the IRS installed high performance infrastructure elements to its Electronic Fraud Detection System (EFDS). Supporting database software was updated to current versions in July 2011. These enhancements improve the system's ability to scan new returns for fraud more quickly and handle inventory more effectively. Additional analytics capabilities are planned in 2014 and the entire IRS EFDS system is scheduled for replacement in 2015 provided budget is available.

Q: Can the present system adequately handle the escalating demands of flagging and stopping fraudulent refund claims?

As of November 18, 2011, the IRS fraud detection system stopped $7.69 billion in refund fraud, which represents a 155 percent increase from last year ($3.01 billion). Annual system updates allow the IRS to identify suspicious refund returns for known types of fraud. Budget permitting, the planned delivery of an EFDS replacement would enable more returns (cases) to be identified and worked due to systemic efficiencies and process automation. Additional flexibility in the replacement system would reduce the percentage of non-fraudulent refund claims frozen by the IRS, enable real-time rather than annual response to trends, and enhance IRS capabilities to detect, resolve, and prevent criminal and civil non-compliance thereby reducing issuance of fraudulent tax refunds.

Q: How would budget cuts affect an Information Systems upgrade and the IRS's ability to carry out its core mission of tax collection and enforcement?

The IRS continues to make significant progress on modernization. This forward progress is critical to the long-term success of IRS efforts to reduce the tax gap, improve taxpayer service, and reduce operating costs. However, with additional budget cuts, the IRS would have to look at all available options, including prioritization of limited resources so that existing systems can be maintained to

prevent system failure, which would have significant impact on taxpayer service and enforcement efforts.

The IRS relies on more than 200 complex legacy IT systems to support tax filing, collections, assessments, and enforcement programs. Technology investments are critical to support IRS programs such as those addressing taxpayer identity theft and fraud. With available resources, the IRS will continue to invest in IT systems to:

- Protect and prevent unauthorized access to taxpayer information and address security vulnerabilities.
- Upgrade technology for security tools to protect IRS-wide systems and taxpayers.
- Advance use of tools for data mining, analytics, reporting, and case building.
- Make progress on the transition from a paper-based to an electronic-based environment.
- Provide uninterrupted year-round access to tax processing systems.

Q: How would human resources reductions affect the efficiency of the IT system?

The IRS's information technology organization has been making strides to adopt industry best practices for IT service delivery and applications development. These practices have led to increased employee productivity and have helped the IRS reduce the need to hire contractors to augment IRS IT staff. However, while we have gained efficiencies, reductions both in human resources and in non-labor budget allocations will strain the IRS's ability to deliver IT services at service levels needed to support the IRS core mission of service, tax collection and enforcement.

Non-critical processes will need to be deferred or, in some cases, curtailed and will ultimately decrease the amount of revenue collected. Because information technology plays an increasingly larger role in the administration of the nation's tax system and, in many cases, directly impacts the taxpayer's user experience, human resource and/or budget reductions in the IRS IT organization will have a demonstrable negative impact on the ability of the IRS to carry out its core mission.

Question 2:

The testimony indicates that once an identity thief files a tax return using another person's name and social security number, that this fraudulent return is protected from disclosure by IRS Code section 6103. Even after the fraud is confirmed, victims will no doubt find it outrageous that the IRS cannot release information about the crime unless the identity thief gives their consent. IRS cannot release information even to state or

local law enforcement that may be investigating or prosecuting the identity theft crime under a state criminal statute. Each of the offices represented the hearing has to deal with this law.

Q: Why is this law that was enacted to deal with crimes from 40 years ago still preventing the prosecution of new, escalating criminal schemes?

Section 6103 remains an important safeguard for the confidentiality of taxpayer information. As noted below, we do not think it prevents the Service's efforts to detect, investigate and recommend for prosecution new identity theft schemes and to provide victim assistance.

Prior to 1977, taxpayer information was open to inspection under Treasury regulations approved by the President or under presidential order. Under this regime, the rules regarding disclosure were essentially left to the discretion of the Executive branch. By the mid-1970's, there was increased Congressional and public concern about the widespread use of tax information by government agencies for purposes unrelated to tax administration. This concern culminated with a total revision of section 6103 in the Tax Reform Act of 1976. There, Congress eliminated Executive discretion regarding what information could be disclosed to which Federal and state agencies and established a new statutory scheme under which taxpayer information was confidential and not subject to disclosure except to the extent explicitly provided by the Code. Although there have been many amendments to the law since that time, the basic statutory regime established in 1976 remains in place today.

We recognize that when section 6103 was enacted 35 years ago, the internet was not yet born. Yet it remains the law governing the disclosure of taxpayer information and its application to the vastly different threats to taxpayer privacy and information security, which exists in today's world, can be challenging. Nevertheless, the Service's view is that the victim of a fraudulently filed return does have access to that return and can legally consent to its release to local law enforcement. It is not the thief who must consent. Unfortunately, we have learned that some confusion exists on this issue. We have asked our Office of Chief Counsel to provide advice that clarifies the law concerning how IRS campuses and field offices should handle requests from identity theft victims for copies of such returns and the ability of the Service to notify other law enforcement agencies upon the discovery of these fraudulent returns. We expect that this will enhance the Service's efforts to combat identity theft.

Q: What would be an appropriate legislative response to certain section 6103 provisions that can enable you to do your job of stopping these crimes more effectively?

We believe that our current efforts to combat identity theft can accommodate the still-important confidentiality protections of section 6103 while vigorously pursuing

cases of identity theft. We have recently initiated discussions with our state revenue agency partners to explore how we may collaborate on combating these identity theft schemes. We intend to clarify ways in which we can share taxpayer information with other law enforcement authorities.

Q: Has there been proposals from any of your offices on adjusting Section 6103 to meet the needs of your agencies in combating identity theft crimes?

Yes, we support making section 6103(k)(10), which allows us to share information with prison officials, permanent. This provision is set to expire at the end of 2011.

Q: What consequences, both negative and positive, would such a legislative remedy have?

Whenever consideration is given to proposing an amendment to section 6103, there must be a balance between the need for the information and the related impact the disclosure would have on compliance with our country's voluntary assessment system. Thus, a balance must be struck that allows law enforcement to do work Congress believes is vital while not eroding the public's view that they can be forthcoming in their disclosures to the IRS.

Question 3

Compared to the over half million cases of ID theft tax refund fraud cases identified by IRS, approximately 245 cases ended up being prosecuted by DOJ in 2010. State and local law enforcement agencies are typically the first agencies to receive information from taxpayers when an identity theft is discovered. However, IRS records become critical to the investigation and prosecution of these cases, once the ID theft progresses to tax refund or employment fraud. Many of these cases cannot be investigated by state and local law enforcement because IRS cooperation is limited by Internal Revenue Code section 6103.

Q: Please explain the reason for the low levels of prosecution of these cases?

In FY 2011, Criminal Investigation (CI) special agents applied over 225,000 hours to identity theft related investigations, an increase over FY 2009 and FY 2010 levels. Prosecution recommendations, which increased by approximately 48% over FY 2010 and 140% over FY 2009, were made on 218 investigations involving over 34,000 false tax returns. In many of these instances a limited number of defendants were responsible for multiple false returns. Because of the limited number of special agents, and the other significant program areas of criminal enforcement, the IRS must devote resources to the perpetrators of schemes impacting numerous individuals and involving significant amounts of fraud. The incarceration rate on cases sentenced in FY 2011 was 100% with an

average sentence of 44 months, maximizing the deterrent effect for this type of crime. The IRS currently has 259 open identity theft criminal investigations. These investigations (schemes) are developed in our Scheme Development Centers. When they appear to contain sufficient evidence targeting a perpetrator, they are assigned to a field office to perfect the criminal case and recommend prosecution. The actual prosecution of the cases is handled by the United States Attorney's Offices and Tax Division prosecutors. The Department of Justice sets priorities to enforce all federal criminal statutes, including identity theft. While each prosecution may only involve a single defendant or a small group of defendants, in the majority of cases, the number of incidents and victims is significantly greater. Regardless of the number of victims or the amount of the refund involved, the Department of Justice evaluates the merits of each case to determine whether a crime can be proven beyond a reasonable doubt. However, not all incidents of identity theft involve evidence sufficient for prosecution or sufficient evidence to determine the perpetrator. Despite these limitations, the IRS will increase the level of resources used to investigate possible identity theft, and is working hand in hand with DOJ as we increase or filing season work in this area. Notwithstanding this reality, the IRS will increase the priority of identity theft prosecutions and is working hand in hand with DOJ as we increase our filing season work in this area.

Q: What initiatives have been implemented to coordinate with local law enforcement when the tax fraud also involves state tax violations?

The IRS participates in various federal task forces across the country with federal, state, and local law enforcement, which result in federal prosecutions. The IRS participates in approximately 20-25 task forces throughout the country that are concerned with identity theft. In six field offices throughout the Southeast, IRS is participating in identity theft task forces. Currently IRS is participating in identity theft task forces in Florida and Virginia. In Georgia, Alabama, Tennessee and Mississippi, the IRS is seeking to establish or join identity theft task forces. In each of these, IRS Special Agents participate in multi-agency groups of law enforcement officials whose purpose is to address and combat identity theft. These groups and task forces provide a multi-faceted approach, applying a variety of statutes to punish using the different violations applicable to those who steal and misuse identifying information. IRS CI special agents have increased efforts focusing on those committing identity theft related refund fraud.

In addition, the IRS is exploring ways in which our information sharing agreements with our state taxing agency partners can incorporate identity theft indicators and other indicia. Information sharing agreements with some state correctional authorities are another mechanism currently in place.